BAB II
PROFIL INSTANSI TEMPAT MAGANG

2.1 Sejarah Singkat Perusahaan

PT Sekuriti Siber Indonesia adalah sebuah perusahaan konsultan keamanan siber yang berdiri sejak tahun 2017 dan berbasis di Jakarta. Perusahaan ini berfokus pada penyediaan berbagai layanan keamanan siber yang mencakup *penetration testing*, *security assessment*, *compliance security*, *security monitoring*, dan *security training*. Sejak awal berdirinya, PT Sekuriti Siber Indonesia memiliki tujuan untuk membantu berbagai organisasi dan perusahaan dalam meningkatkan ketahanan digital mereka terhadap ancaman dan serangan siber yang kian kompleks dan terus berkembang.

Dengan pengalaman dan dedikasi yang kuat, PT Sekuriti Siber Indonesia telah berkontribusi dalam mengamankan banyak aplikasi yang digunakan secara luas, sehingga membantu menurunkan risiko kerentanan dan mencegah aplikasi-aplikasi tersebut masuk ke dalam daftar aplikasi rentan atau terdampak serangan.

2.2 Visi dan Misi Perusahaan

Visi:

Menjadi perusahaan keamanan siber yang diakui secara global, meningkatkan standar keamanan siber di Indonesia, dan membina generasi baru yang terampil dan berintegritas.

Misi:

1. Memberikan solusi keamanan siber berkualitas tinggi Menyediakan solusi inovatif untuk melindungi organisasi dan individu dari ancaman siber yang terus berkembang.
2. Meningkatkan kesadaran keamanan siber: Melalui edukasi, lokakarya, dan pelatihan, perusahaan berkomitmen untuk meningkatkan pengetahuan masyarakat mengenai pentingnya keamanan siber.
3. Mengembangkan talenta keamanan siber: Memberikan kesempatan

karir dan pengembangan keahlian melalui program magang dan bimbingan profesional.

4. Membangun kemitraan strategis: Menjalin kerja sama dengan pemerintah, organisasi swasta, dan institusi pendidikan untuk memperkuat ekosistem keamanan siber nasional.
5. Menjunjung tinggi etika dan integritas: Mengedepankan transparansi, kepatuhan hukum, dan tanggung jawab sosial dalam setiap lini bisnis dan operasional.

2.3 Layanan Utama PT Sekuriti Siber Indonesia

Untuk mendukung misi dalam meningkatkan keamanan digital di berbagai sektor, PT Sekuriti Siber Indonesia menyediakan beberapa layanan utama, yaitu:

1. Penetration Testing (Pengujian Penetrasi)
   Layanan ini bertujuan untuk mengidentifikasi dan mengevaluasi celah keamanan pada sistem atau aplikasi dengan mensimulasikan serangan siber nyata. Tim melakukan pengujian dari sisi internal maupun eksternal, agar organisasi memahami potensi risiko yang ada.
2. Security Assessment (Penilaian Keamanan)
   Melakukan evaluasi komprehensif terhadap sistem, jaringan, maupun aplikasi untuk mengetahui apakah telah memenuhi standar keamanan yang berlaku, seperti OWASP, ISO 27001, maupun PCI DSS. Hasil *assessment* digunakan sebagai dasar perbaikan dan penguatan keamanan.
3. Security Operation Center (SOC)
   Menyediakan layanan pemantauan keamanan 24/7 melalui pusat operasi keamanan yang dilengkapi dengan SIEM *(Security Information and Event Management)* untuk mendeteksi, menganalisis, dan merespons ancaman siber secara real-time.
4. System Hardening
   Layanan ini berfokus pada penguatan sistem TI agar lebih tahan terhadap serangan siber, dengan cara menghapus konfigurasi yang

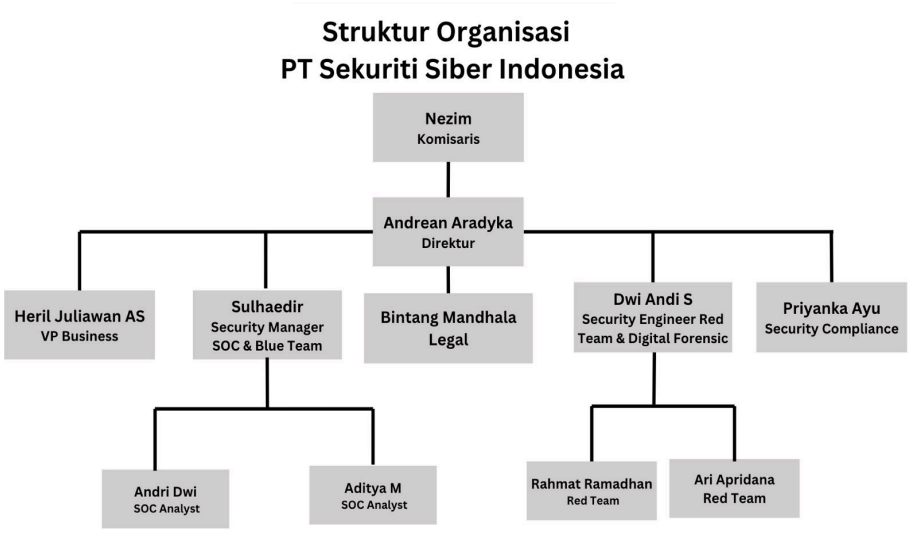
tidak aman, memperbarui *patch* keamanan, serta menerapkan kontrol akses yang ketat.

5. Digital Forensic (Forensik Digital)

   Menyediakan layanan investigasi insiden siber dengan cara mengumpulkan, menganalisis, dan melaporkan bukti digital yang valid. Layanan ini sangat penting untuk menangani kasus pelanggaran data, kebocoran informasi, maupun kejahatan siber lainnya.

2.4 Struktur Organisasi

Struktur organisasi di bawah ini dibentuk oleh Nemo Security pada tahun 2017, dan disahkan secara aklamasi menjadi PT. Sekuriti Siber Indonesia pada tahun 2018, dengan susunan organisasi sebagai berikut:



Gambar 2. 1 Struktur Organisasi

Struktur organisasi di PT Sekuriti Siber Indonesia dipimpin oleh seorang Komisaris, yang berperan sebagai pengawas dan penentu arah strategis perusahaan. Komisaris bertanggung jawab dalam memastikan bahwa seluruh kegiatan perusahaan berjalan sesuai dengan visi dan misi yang telah ditetapkan. Di bawah Komisaris, terdapat Direktur yang memiliki peran sentral dalam mengelola dan mengkoordinasikan seluruh aktivitas operasional perusahaan secara menyeluruh. Direktur ini membawahi beberapa divisi

utama yang masing-masing memiliki peran dan tanggung jawab yang spesifik, yaitu:

1. VP Business, yang berfokus pada pengembangan bisnis, pengelolaan relasi dengan klien, serta ekspansi layanan dan peluang pasar baru.
2. Security Manager SOC (Security Operation Center), yang bertanggung jawab atas pengawasan keamanan siber secara real-time, termasuk mendeteksi, menganalisis, dan merespons ancaman keamanan yang mungkin terjadi.
3. Divisi Legal, yang mengatur segala aspek hukum, mulai dari kontrak, kepatuhan terhadap peraturan, hingga penyelesaian permasalahan hukum terkait insiden keamanan informasi.
4. Security Engineer Red Team & Digital Forensic, divisi yang memiliki dua peran vital yaitu melakukan simulasi serangan siber melalui Red Team untuk menguji ketahanan sistem, serta melakukan analisis forensik digital guna mengungkap dan menangani insiden keamanan.

Setiap divisi menjalankan fungsi dan perannya masing-masing, namun tetap saling berkolaborasi dalam rangka menjaga keamanan dan keberlangsungan bisnis perusahaan. Keterpaduan antar divisi inilah yang memungkinkan PT Sekuriti Siber Indonesia untuk memberikan layanan keamanan siber yang komprehensif, profesional, dan sesuai dengan kebutuhan klien di era digital yang penuh ancaman seperti saat ini.

2.5 Budaya dan Nilai Perusahaan

PT Sekuriti Siber Indonesia menjunjung tinggi budaya kerja yang mengutamakan integritas, inovasi, dan profesionalisme. Selain itu, perusahaan ini juga aktif mendorong pengembangan talenta muda melalui program magang dan pelatihan yang bertujuan mencetak generasi profesional keamanan siber yang andal dan beretika.

Selain sebagai penyedia layanan, perusahaan ini juga memiliki misi sosial melalui kegiatan edukasi publik mengenai keamanan digital agar masyarakat Indonesia lebih peka dan sadar terhadap potensi ancaman di dunia maya.