BAB II
PROFIL INSTANSI TEMPAT MAGANG

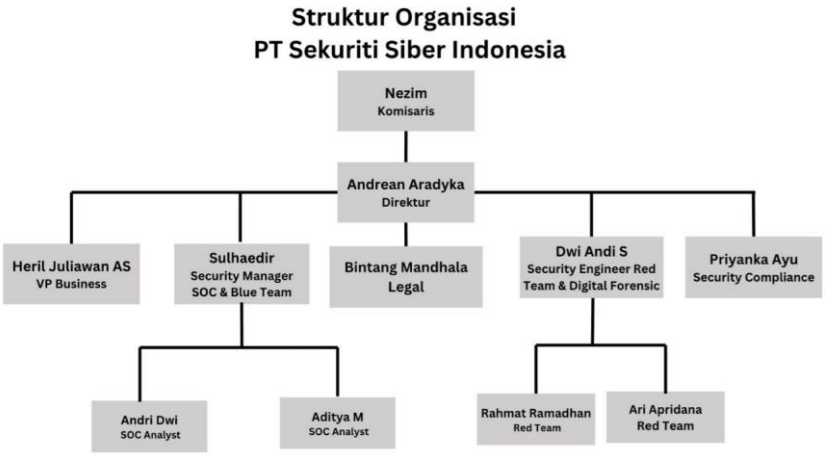
2.1. Sejarah PT Sekurity Siber Indonesia (Nemo Security)

PT Sekuriti Siber Indonesia (Nemo Security) adalah perusahaan konsultan keamanan *siber* yang berfokus pada layanan pengujian penetrasi, penilaian keamanan, kepatuhan keamanan, pemantauan keamanan, serta pelatihan keamanan. Berdiri sejak tahun 2017, perusahaan ini telah mengembangkan portofolio layanan yang komprehensif untuk mendukung keamanan banyak aplikasi yang digunakan secara luas, sehingga membantu melindungi mereka dari daftar kerentanan yang berpotensi disebarkan.

Spesialisasi dalam pengujian penetrasi, penilaian kerentanan, penilaian aplikasi web, respons insiden, *forensik digital*, pemantauan keamanan, pemantauan *SIEM (Security Information and Event Management)*, intelijen ancaman, serta kepatuhan terhadap standar keamanan internasional *seperti ISO (Information Security Management System)* 27001 dan *PCI DSS (Payment Card Industry Data Security Standard)*, Sekuriti Siber Indonesia juga memberikan perhatian pada aspek privasi data. Sebagai perusahaan yang bergerak di industri Jasa *TI (Information Technology) dan Konsultan TI (Information Technology)*.

2.2. Struktur Organisasi PT Sekurity Siber Indonesia (Nemo Security)

Struktur Organisasi mencerminkan di mana setiap individu memiliki peran dan tanggung jawab yang spesifik untuk mendukung keamanan *siber* secara menyeluruh.



Gambar 2. 1 Sturktur Organisasi PT Sekurity Siber Indonesi (Nemo Security)

Dengan struktur organisasi yang dijabarkan dibawah ini :

1. Nezim – Komisaris

   Bertugas mengawasi jalannya perusahaan dan memberikan arahan strategis kepada direktur.

2. Andrean Aradyka – Direktur

   Bertanggung jawab atas pengelolaan dan operasional perusahaan secara keseluruhan, memastikan visi dan misi perusahaan terlaksana.

3. Heril Juliawan *AS - VP Business*

   Bertanggung jawab untuk mengelola aspek bisnis perusahaan, termasuk pengembangan strategi bisnis dan hubungan dengan mitra.

4. Sulhaedir - *Security Manager (SOC & Blue Team)*

   a. Mengawasi operasional keamanan di *Security Operations Center (SOC)* dan *Blue Team*, yang fokus pada pertahanan dan perlindungan sistem dari ancaman keamanan.
   b. Memiliki dua staf Andri Dwi dan Aditya M sebagai *SOC Analyst.*

5. Bintang Mandhala – Legal

   Bertanggung jawab atas segala aspek hukum perusahaan, termasuk kepatuhan terhadap regulasi dan penyelesaian sengketa.

6. Dwi Andi S - *Security Engineer (Red Team & Digital Forensic)*

   a. Bertugas melakukan pengujian keamanan (simulasi serangan) serta *forensik digital* untuk menganalisis dan memitigasi insiden *siber*.
   b. Memiliki dua anggota Rahmat Ramadhan dan Ari Apridana sebagai *Red Team*

7. Priyanka Ayu - *Security Compliance*

   Bertugas memastikan bahwa perusahaan mematuhi regulasi dan standar keamanan *siber* yang berlaku.

2.3. Visi dan Misi PT Sekurity Siber Indonesia (Nemo Security)

Visi PT Sekurity Siber Indonesia (Nemo Security) adalah Menjadi perusahaan keamanan *siber* yang diakui secara global, meningkatkan standar keamanan *siber* di Indonesia, dan membina generasi baru profesional keamanan *siber* yang terampil dan berintegritas.

Untuk mewujudkan visi tersebut, PT Siber Sekurity Indonesia (Nemo Security) memiliki misi sebagai berikut:

1. Memberikan solusi inovatif untuk melindungi dari ancaman *siber*.
2. Memberikan pendidikan dan lokakarya gratis untuk meningkatkan pengetahuan keamanan siber.
3. Menawarkan peluang karier melalui magang dan bimbingan.
4. Berkolaborasi dengan pemerintah dan organisasi untuk memperkuat keamanan *siber*.
5. Menjaga transparansi, etika, dan kepatuhan dalam semua operasi.

2.4. Tugas Pokok dan Fungsi PT Sekurity Siber Indonesia (Nemo Security)

Melakukan identifikasi dan analisis terhadap celah keamanan pada infrastruktur teknologi yang digunakan oleh instansi. Tugas ini mencakup menemukan potensi kerentanan seperti input yang tidak divalidasi, konfigurasi keamanan yang lemah, serta celah lain yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Selain itu, juga bertanggung jawab untuk menganalisis tingkat risiko yang dihadapi oleh sistem, termasuk potensi pencurian data, penyusupan, hingga gangguan operasional yang dapat merugikan instansi.

Fungsi utama yaitu melindungi data sensitif, seperti informasi internal atau dokumen penting instansi, guna mencegah pelanggaran data yang dapat merusak reputasi dan kepercayaan publik. Selain itu, dengan menemukan dan memperbaiki kerentanan yang ada, instansi dapat meminimalkan risiko kerugian finansial akibat pencurian data, kehilangan pelanggan, atau biaya pemulihan setelah terjadinya serangan *siber*.

Dengan melaksanakan tugas pokok dan fungsi keamanan siber instansi melalui langkah preventif yang bertujuan memastikan operasional berjalan lancar dan aman dari ancaman siber.