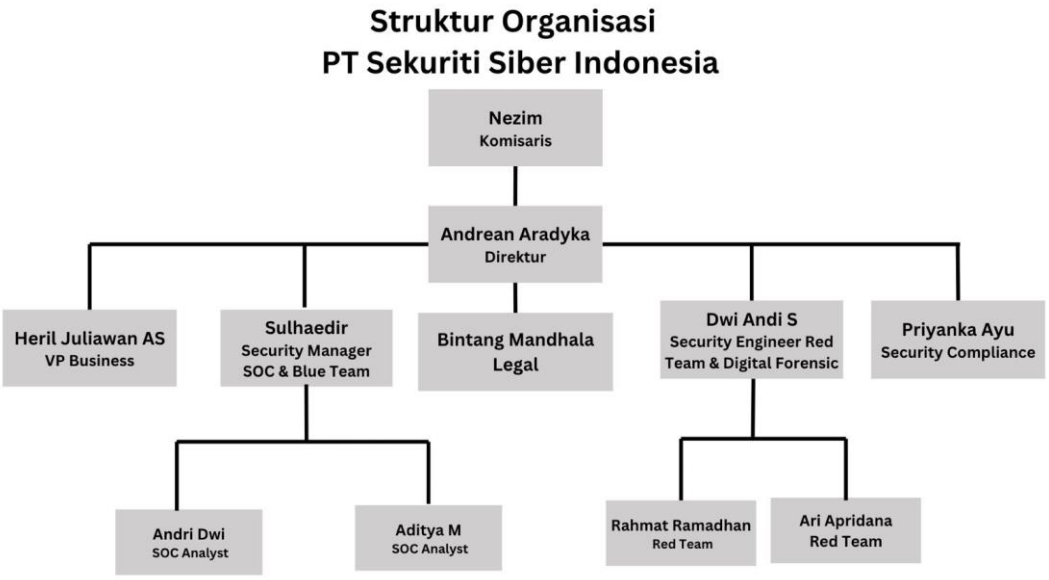
BAB II
PROFIL INSTANSI TEMPAT MAGANG

2.1 Sejarah

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)*.



Gambar 1 Struktur Organisasi

2.2 Visi dan Misi

Visi:

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.

Visi ini mencerminkan tujuan jangka panjang organisasi untuk menjadi pemimpin global dalam bidang keamanan *siber*. Hal ini tidak hanya berfokus pada keberhasilan di dalam negeri, tetapi juga mencakup pengakuan internasional. Dengan meningkatkan standar keamanan *siber* di Indonesia, perusahaan ingin menciptakan lingkungan *digital* yang lebih aman dan berdaya saing tinggi. Selain itu, pembinaan generasi baru yang terampil dan berintegritas menunjukkan komitmen perusahaan dalam memastikan keberlanjutan tenaga ahli di bidang ini.

Misi:

1. Keamanan Siber Berkualitas Tinggi: Menyediakan solusi inovatif untuk melindungi dari ancaman siber.
2. Meningkatkan Kesadaran: Memberikan pendidikan dan pelatihan gratis untuk meningkatkan pengetahuan keamanan siber.
3. Mengembangkan Talenta: Menawarkan peluang karier melalui magang dan bimbingan. Kemitraan Strategis:
4. Bekerjasama dengan pemerintah dan organisasi untuk memperkuat keamanan siber.
5. Etika dan Integritas: Menjaga transparansi, etika, dan kepatuhan dalam semua operasi.

2.3 Struktur Organisasi

Komisaris

Sebagai komisaris, memiliki tanggung jawab atas pengawasan strategis perusahaan. Memiliki tugas :

1. Menetapkan visi dan misi perusahaan.
2. Mengawasi kinerja perusahaan dan memberikan arahan kepada direktur.
3. Menjaga kepentingan pemegang saham dan memastikan perusahaan berjalan sesuai tujuan strategis.
4. Memberikan evaluasi terhadap laporan dari direktur dan manajemen.

Direktur

Direktur memegang peran sentral dalam memimpin dan mengelola operasional perusahaan sehari-hari. Memiliki tugas :

1. Mengambil keputusan strategis untuk memastikan keberlangsungan dan pertumbuhan perusahaan.
2. Mengkoordinasikan seluruh divisi untuk bekerja secara efektif.
3. Bertanggung jawab atas perencanaan, pelaksanaan, dan evaluasi strategi perusahaan.
4. Memastikan setiap proyek berjalan sesuai target waktu dan anggaran.
5. Memberikan laporan berkala kepada komisaris.

VP Business

Sebagai *Vice President Business*, memiliki tugas dalam pengembangan bisnis perusahaan. Memiliki tugas :

1. Mengembangkan strategi bisnis untuk menarik klien dan mitra baru.
2. Menjalin dan menjaga hubungan baik dengan pelanggan dan stakeholder.
3. Memonitor kinerja bisnis dan mengevaluasi hasilnya.
4. Menganalisis tren pasar dan peluang bisnis baru.
5. Membuat kebijakan dan perencanaan strategis dalam mendukung pertumbuhan perusahaan.

Security Manager SOC & Blue Team

Security Manager memimpin tim *Security Operations Center (SOC)* dan *Blue Team,* yang berfokus pada pertahanan keamanan *siber* perusahaan. Memiliki tugas:

1. Mengelola SOC untuk memantau keamanan jaringan, server, dan infrastruktur perusahaan.
2. Menangani insiden keamanan, termasuk deteksi, analisis, dan mitigasi ancaman.
3. Memimpin tim *Blue Team* untuk merancang sistem keamanan yang kuat dan mencegah serangan.
4. Menjalankan penilaian risiko dan membuat kebijakan keamanan *siber*.
5. Berkolaborasi dengan *Red Team* untuk mengidentifikasi kelemahan keamanan.

Anggota tim dibawah Security Manager

1. SOC Analyst 1 :
    a. Memantau aktivitas keamanan sistem menggunakan tools monitoring.
    b. Mengidentifikasi *anomali* dan mengirimkan laporan insiden keamanan.
    c. Melakukan analisis log dan menyelesaikan peringatan keamanan.
2. SOC Analyst 2 :
    a. Mengelola sistem keamanan *siber* perusahaan dan menangani eskalasi insiden.

b. Menganalisis data dan mengidentifikasi ancaman *siber* yang potensial.

c. Memberikan rekomendasi perbaikan risiko keamanan.

Legal

Sebagai divisi legal, memiliki tugas mendukung perusahaan dari aspek hukum. Memiliki tugas :

1. Menyediakan dukungan hukum dalam semua aktivitas perusahaan.
2. Menyusun dan meninjau kontrak bisnis, kebijakan internal, serta perjanjian dengan mitra.
3. Menangani permasalahan hukum yang terkait dengan keamanan siber dan bisnis.
4. Memberikan nasihat hukum untuk memastikan kepatuhan terhadap regulasi yang berlaku.
5. Menjaga perusahaan dari risiko litigasi.

Security Engineer Red Team & Digital Forensic

Security Engineer memimpin *Red Team* dan *Digital Forensic*, yang bertanggung jawab untuk pengujian keamanan dan investigasi *siber*. Memiliki tugas:

1. Melakukan pengujian penetrasi *(pentesting)* untuk menemukan kerentanan dalam sistem perusahaan.
2. Menjalankan simulasi serangan untuk mengevaluasi kekuatan pertahanan

Blue Team.

3. Membuat laporan kelemahan keamanan dan memberikan solusi perbaikan.
4. Menyelidiki insiden *siber*, menganalisis jejak *digital*, dan mengumpulkan bukti forensik.
5. Memberikan laporan hasil investigasi insiden keamanan kepada manajemen.

Anggota tim dibawah Security Engineer :

1. *Red Team* 1 :
   a. Melakukan pentesting terhadap aplikasi, jaringan, dan sistem.
   b. Mengevaluasi sistem keamanan dengan pendekatan ofensif.
   c. Menyusun laporan hasil pengujian dan rekomendasi keamanan.
2. *Red Team* 2 :
   a. Menjalankan eksploitasi kelemahan keamanan dalam simulasi serangan.
   b. Membantu dalam menemukan celah keamanan yang belum diketahui.
   c. Bekerja sama dengan Blue Team untuk memperbaiki kerentanan.

Security Compliance

Sebagai *Security Compliance*, memiliki fokus pada kepatuhan kebijakan keamanan *siber* perusahaan. Memiliki tugas :

1. Menyusun, mengimplementasikan, dan mengawasi kebijakan keamanan *siber*.

2. Melakukan audit internal dan eksternal untuk memastikan kepatuhan terhadap standar keamanan.
3. Mengidentifikasi risiko keamanan yang berpotensi menyalahi kebijakan.
4. Mengedukasi karyawan tentang pentingnya keamanan siber dan kepatuhan.
5. Menyusun laporan kepatuhan untuk manajemen dan stakeholder.