BAB II
PROFIL INSTANSI TEMPAT MAGANG

2.1 Latar Belakang PT Sekuri Siber Indonesia (Nemo Sekuriti)

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 Visi dan Misi PT Sekuri Siber Indonesia (Nemo Sekuriti)

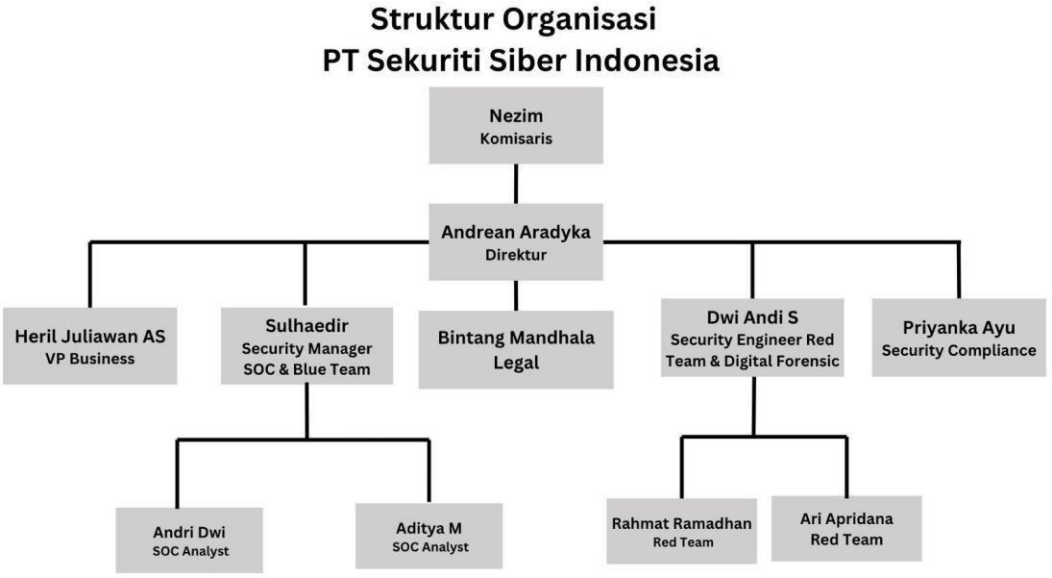
Visi PT Sekuri Siber Indonesia (Nemo Sekuriti) Menjadi perusahaan keamanan siber yang diakui secara global, meningkatkan standar keamanan siber di Indonesia, serta membina generasi baru profesional keamanan siber Yang terampil dan berintegritas.

Untuk mewujudkan visi yang dimiliki oleh PT Sekuri Siber Indonesia (Nemo Sekuriti) maka dari itu untuk mewujudkan visi tersebut dengan menerapkan misi sebagai berikut :

a. Menyediakan solusi inovatif untuk melindungi dari ancaman siber.
b. Memberikan edukasi dan lokakarya gratis untuk meningkatkan pengetahuan tentang keamanan siber.
c. Menawarkan peluang karir melalui program magang dan pendampingan.

Bekerja sama dengan pemerintah dan organisasi untuk memperkuat keamanan siber. Mempertahankan transparansi, etika, dan kepatuhan dalam seluruh operasi.

2.3 Struktur Organisasi PT Sekuri Siber Indonesia (Nemo Sekuriti)



Gambar 2. 3 Struktur Organisasi PT Siber Sekuriti Indonesia(nemo sekuriti)

1) Nezim sebagai Komisaris bertugas mengawasi kinerja perusahaan dan memberikan arahan strategis kepada direksi untuk memastikan bahwa perusahaan berjalan sesuai dengan visi dan misinya.

2) Andrean Aradyka sebagai Direktur bertanggung jawab untuk menjalankan operasional perusahaan secara keseluruhan, termasuk mengelola sumber daya, mengambil keputusan strategis, dan memimpin tim di bawahnya.

3) Heril Juliawan AS sebagai VP Business Bertanggung jawab atas pengelolaan aspek bisnis perusahaan, seperti pengembangan bisnis, hubungan pelanggan, dan strategi pemasaran.

4) Sulhaedir Sebagai Security Manager SOC & Blue Team

a. Mengelola operasi keamanan (SOC) dan tim Blue Team dan fokus pada

pertahanan jaringan dan pemantauan untuk mencegah serangan siber.

b. Memiliki dua staf yaitu Andri Dwi dan Aditya M sebagai SOC Analyst yang bertugas Menganalisis aktivitas jaringan untuk mendeteksi dan merespons ancaman.

5) Bintang Mandhala sebagai bagian legal bertugas Menangani aspek hukum perusahaan, termasuk kepatuhan terhadap regulasi, kontrak bisnis, dan perlindungan hukum.

6) Dwi Andi S Sebagai Security Engineer Red Team & Digital Forensic

a. Memimpin tim Red Team (pengujian keamanan melalui simulasi serangan) dan Digital Forensic dan bertanggung jawab untuk mengidentifikasi kelemahan sistem dan menganalisis bukti digital pasca-insiden.

b. Memiliki dua anggota yaitu Rahmat Ramadhan dan Ari Apridana sebagai Red Team.

7) Priyanka Ayu Sebagai Security Compliance Bertugas memastikan bahwa perusahaan mematuhi standar keamanan siber, regulasi, dan kebijakan terkait.

2.4 Tools Pengujian Keamanan Website

Burp Suite adalah salah satu alat *penetration testing* yang sangat populer dan banyak digunakan oleh para profesional keamanan siber untuk menguji keamanan aplikasi web. Alat ini dikembangkan oleh *PortSwigger* dan dirancang untuk membantu menemukan, menganalisis, dan mengeksploitasi kerentanan dalam aplikasi web . berikut penjelasan fitur pada *tools burpsuite*:

a. *Intercept Proxy* Fitur utama *Burp Suite* adalah *proxy* yang memungkinkan pengguna untuk mencegat dan memodifikasi permintaan (request) dan tanggapan

(response) *HTTP* antara browser dan server. Ini membantu dalam menganalisis dan mengidentifikasi celah keamanan.

b. *Repeater* Digunakan untuk mengirim ulang permintaan *HTTP* secara manual dengan modifikasi tertentu. Sangat berguna untuk mengeksploitasi celah seperti *IDOR, CSRF*, atau validasi input lainnya.

c. Intruder Alat ini digunakan untuk melakukan *brute-force* atau *fuzzing* terhadap input parameter, seperti mencoba kombinasi password, parameter ID, atau input data lainnya untuk mencari celah.

d. *Scanner (Pro Version) Burp Suite Professional* dilengkapi dengan scanner otomatis untuk mendeteksi kerentanan umum seperti *SQL Injection, Cross-Site Scripting (XSS),* dan lainnya.

e. *Decoder* Fitur ini memungkinkan pengguna untuk mendekode dan mengenkripsi data, seperti Base64, URL-encoding, dan lainnya.

f. *Comparer* Membandingkan dua set data (seperti response HTTP) untuk menemukan perbedaan yang mungkin menunjukkan celah keamanan.

g. *Extensibility Burp Suite* mendukung ekstensi tambahan yang dibuat dengan bahasa pemrograman Python atau Java melalui API Burp Extender. Ini memberikan fleksibilitas untuk menambahkan fitur sesuai kebutuhan pengguna.