BAB II
TINJAUAN UMUM TEMPAT KERJA PROFESI

2.1 Sejarah Perusahaan

Dimulai pada tahun 2010, melalui kemitraan strategis NOOSC kini telah menjadi layanan keamanan terkelola pilihan di Indonesia yang melayani beberapa lembaga keuangan dan jasa terbesar di negara ini. Perusahaan ini beroperasi pada Pusat Operasi Keamanan 24x7 khusus dengan perlindungan pemulihan bencana Profesional ahli, kredensial & catatan internasional yang dapat diverifikasi Praktik terbaik, proses pengiriman yang digerakkan oleh tingkat layanan (sesuai dengan ISO27001) Investasi R&D aktif yang mencakup ancaman & teknologi keamanan baru yang muncul.

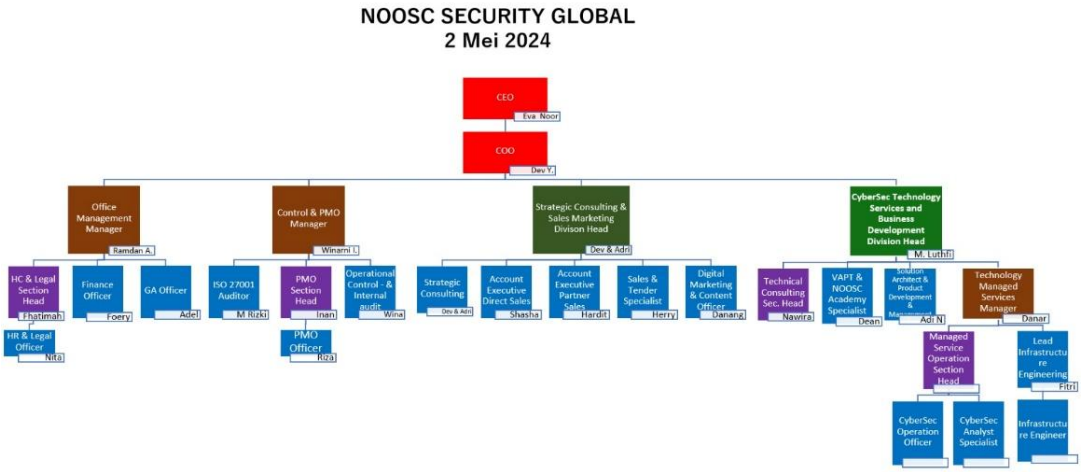
Gambar 2. 1 Logo Perusahaan NOOSC
Sumber: Dokumen Internal NOOSC

2.2 Struktur Organisasi

Struktur organisasi ini memberikan gambaran yang jelas tentang pembagian tugas dan tanggung jawab di dalam perusahaan. Berikut adalah penjelasan singkat dari setiap departemen dan posisinya terlihat pada **Gambar 2. 2**:

Tingkat Tertinggi:

- **CEO**: Merupakan pemimpin tertinggi perusahaan dan bertanggung jawab atas visi, misi, dan strategi keseluruhan perusahaan.
- **COO**: Bertanggung jawab atas operasi sehari-hari perusahaan, memastikan semua departemen berjalan efisien dan efektif.



Gambar 2. 2 Struktur Organisasi Perusahaan NOOSC
Sumber: Dokumen Internal NOOSC

Tingkat Manajemen:

- **Office Management**: Mengelola administrasi umum perusahaan.
- **Control & PMO**: Mengelola proyek dan memastikan proyek berjalan sesuai rencana.
- **Strategy, Consulting & Sales Marketing Division Head**: Bertanggung jawab atas strategi bisnis, konsultasi, penjualan, dan pemasaran.
- **CyberSec Technology, Services and Business Development Division Head**: Bertanggung jawab atas pengembangan teknologi keamanan siber, layanan, dan pengembangan bisnis di bidang ini.

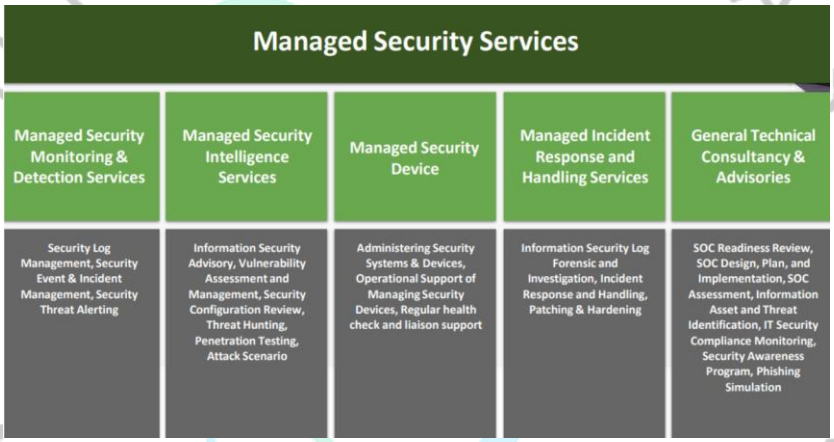
Departemen dan Posisi:

- **HR & Legal Section**: Mengelola sumber daya manusia dan urusan hukum perusahaan.
- **Finance**: Mengelola keuangan perusahaan.
- **ISO 27001 Auditor**: Bertanggung jawab atas audit sistem manajemen keamanan informasi.
- **PMO Officer**: Mengelola proyek-proyek khusus.
- **Operational Control**: Mengontrol operasi sehari-hari.
- **Strategic Consulting**: Memberikan konsultasi strategis.
- **Account Executive Direct Sales**: Bertanggung jawab atas penjualan langsung.

- **Account Executive Partner**: Bertanggung jawab atas penjualan melalui mitra.
- **Sales & Tendering**: Mengelola penjualan dan tender.
- **Digital Marketing & Content**: Mengelola pemasaran digital dan konten.
- **Technical Security**: Mengelola keamanan teknis.
- **Product & Solutions Architect**: Profesional yang bertanggung jawab untuk merancang dan mengembangkan solusi teknologi dan produk yang memenuhi kebutuhan bisnis dan pengguna.
- **Manage Service Operation Section Head**: Posisi manajerial dalam organisasi yang bertanggung jawab untuk mengelola dan mengawasi operasi layanan TI, dengan fokus pada penyampaian layanan yang efisien dan efektif kepada pelanggan.
- **Security Operation Center Analyst**: Sebuah unit yang bertanggung jawab untuk memonitor, mendeteksi, dan merespons insiden keamanan siber dalam suatu organisasi.
- **Cybersecurity Analyst**: Berperan dalam menjaga keamanan informasi dan melindungi organisasi dari risiko yang terkait dengan ancaman siber. Dengan pengetahuan dan keterampilan yang tepat, mereka dapat mengidentifikasi dan mengatasi risiko, serta berkontribusi pada pengembangan strategi keamanan yang efektif.
- **Cybersecurity Engineer**: Profesional yang bertanggung jawab untuk merancang, membangun, dan mengelola sistem dan infrastruktur keamanan siber dalam suatu organisasi.

2.3 Kegiatan Umum Perusahaan

PT NOOSC Security Global **Gambar 2. 3** menyediakan layanan konsultasi dan profesional dengan profesional keamanan siber berpengalaman yang memberikan keahlian langsung dan memetakan rencana kebutuhan Klien yang mencakup aspek strategi, tata kelola, risiko, kepatuhan, dan jaminan. Dalam memandu dan berkonsultasi dengan organisasi untuk mengidentifikasi kesenjangan dan menyarankan solusi untuk mengisi kesenjangan tersebut guna meningkatkan efisiensi, dan memperkuat postur keamanan dan ketahanan siber berdasarkan praktik terbaik, kerangka kerja keamanan, standar industri, dan yang terpenting dari semuanya belajar dari pengalaman sejauh ini.



Gambar 2. 3 Kegiatan Umum Perusahaan NOOSC
Sumber: Dokumen Internal NOOSC

Managed Security Services (MSS) yang dibagi ke dalam lima kategori utama. Berikut penjelasan lengkap untuk setiap layanan:

1. *Managed Security Monitoring & Detection Services*

Layanan pemantauan secara *real-time* terhadap ancaman keamanan, *incident management*, dan insiden keamanan. Ini membantu organisasi mendeteksi dan merespon ancaman sebelum menjadi masalah besar.

- *Security Log Management*

  Pengelolaan log keamanan yang dihasilkan oleh berbagai sistem dan aplikasi.
- *Security Event & Incident Management*

Penanganan dan pengelolaan kejadian atau insiden keamanan secara terstruktur.

- *Security Threat Alerting*
  Pemberitahuan tentang ancaman atau potensi serangan yang terdeteksi melalui pemantauan.

2. *Managed Security Intelligence Services*

Layanan yang menyediakan informasi mendalam terkait nasihat strategis untuk membantu organisasi mengidentifikasi dan memitigasi potensi kerentanan atau ancaman keamanan. Fokusnya adalah pada penilaian risiko dan respons proaktif terhadap ancaman.

- Information Security Advisory
  Memberikan saran terkait peningkatan keamanan informasi.
- *Vulnerability Assessment and Management*
  Identifikasi dan pengelolaan kerentanan sistem untuk mencegah potensi serangan.
- *Security Configuration Review*
  Tinjauan konfigurasi sistem untuk memastikan keamanan yang optimal.
- *Threat Hunting*
  Proses aktif mencari ancaman keamanan yang tersembunyi dalam jaringan.
- *Penetration Testing*
  Menguji kerentanan sistem dengan mensimulasikan serangan dari luar.
- *Attack Scenario*
  Simulasi serangan untuk menguji kesiapan sistem keamanan.

3. *Managed Security Device*

Layanan ini mencakup pengelolaan dan pemeliharaan perangkat keamanan untuk memastikan perangkat tersebut selalu dalam kondisi optimal. Dukungan operasional rutin membantu menjaga keamanan sistem dan mencegah kerusakan.

- *Administering Security Systems & Devices*
  Pengelolaan perangkat keamanan yang ada di organisasi, termasuk *firewall*, IDS/IPS, dll.
- *Operational Support of Managing Security Devices*
  Memberikan dukungan operasional harian untuk perangkat keamanan.
- *Regular health check and liaison support*
  Memastikan perangkat keamanan berfungsi dengan baik melalui pemeriksaan rutin.

4. Managed Incident Response and Handling Services

Merupakan layanan respons dan penanganan insiden keamanan secara langsung. Proses ini melibatkan investigasi mendalam dan penerapan langkah-langkah untuk menanggulangi serta memitigasi dampak insiden.

- *Information Security Log Forensic and Investigation*
  Melakukan analisis forensik terhadap log untuk mengidentifikasi sumber dan dampak insiden keamanan.
- *Incident Response and Handling*
  Penanganan insiden keamanan secara cepat dan efisien.
- *Patching & Hardening*
  Memperbaiki kerentanan dengan *patch* dan memperkuat sistem dari potensi serangan.

5. *General Technical Consultancy & Advisories*

Layanan konsultasi ini memberikan panduan teknis umum untuk meningkatkan keamanan IT organisasi secara keseluruhan, termasuk pengelolaan tim SOC, penilaian aset informasi, serta pelatihan kesadaran keamanan kepada staf.

- *SOC Readiness Review*
  Menilai kesiapan tim Security Operations Center (SOC) dalam menghadapi ancaman keamanan.
- *SOC Design, Plan, and Implementation*
  Membantu dalam perancangan dan implementasi pusat operasi keamanan.
- *SOC Assessment*
  Evaluasi terhadap kinerja dan efektivitas SOC.
- *Information Asset and Threat Identification*
  Identifikasi aset informasi kritis dan potensi ancaman yang mungkin mempengaruhi mereka.
- *IT Security Compliance Monitoring*
  Memastikan sistem sesuai dengan regulasi dan standar keamanan yang berlaku.
- *Security Awareness Program*
  Melatih staf tentang keamanan informasi dan praktik terbaik untuk menjaga keamanan.
- *Phishing Simulation*
  Simulasi serangan phishing untuk menguji kesiapan dan kewaspadaan staf terhadap serangan siber.

Berbagai layanan *Managed Security Services* yang mengacu pada pemantauan, intelijen, pengelolaan perangkat keamanan, respons insiden, dan konsultasi teknis. Hal ini membantu organisasi dalam melindungi aset informasi mereka, merespons ancaman keamanan dengan cepat, dan memastikan kepatuhan terhadap standar keamanan yang berlaku.