

BAB 2 GAMBARAN UMUM PERUSAHAAN

2.1 Sejarah Singkat Perusahaan



Gambar 2.1. Logo CTI

PT Computrade Technology International (CTI Group) merupakan distributor IT terbesar di Asia Tenggara yang terus berinovasi sejak tahun 2003. CTI Group beroperasi di bidang teknologi informasi dan membawahi sejumlah perusahaan yang menyediakan berbagai solusi IT, Salah satunya adalah PT Defender Nusa Semesta (DEFENXOR).



Gambar 2.2. Logo Defenxor

Defender Nusa Semesta (DNS), yang dikenal dengan merek dagang Defenxor, adalah anak perusahaan CTI yang menyediakan layanan keamanan teknologi informasi (IT Security). PT. Defender Nusa Semesta didirikan pada tahun 2016. Kantor pusat perusahaan berlokasi di Graha BIP Lantai 6, Jl. Jenderal Gatot Subroto Kav. 23, Karet Semanggi, Setiabudi, Jakarta Selatan, DKI Jakarta 12930. Defenxor dipimpin oleh Chief Executive Officer (CEO) Bapak Toto A. Atmojo, serta didukung oleh Chief Technology Officer (CTO) Bapak Memet Anwar [6].

Defenxor menyediakan solusi keamanan teknologi informasi yang sederhana namun efektif. Layanan ini bertujuan untuk membantu berbagai bisnis dalam mengelola keamanan secara menyeluruh, meningkatkan kecepatan dan kualitas respons terhadap insiden, serta memastikan kepatuhan terhadap

berbagai regulasi yang berlaku. Defenxor menawarkan berbagai layanan, meliputi pemantauan keamanan 24/7, manajemen insiden, pengelolaan kerentanan, konsultasi melalui aplikasi mobile, manajemen log, serta pencatatan data jaringan untuk keperluan analisis forensik. Melalui layanan tersebut, Defenxor berkomitmen untuk mendukung kelangsungan operasional bisnis dan melindungi aset digital dari potensi ancaman siber[6].

Defenxor berfokus untuk membantu entitas bisnis dalam melindungi aset digital mereka dengan meningkatkan tingkat keamanan informasi ke level yang lebih tinggi dan sesuai dengan standar industri. Sebagai mitra keamanan dari Computrade Technology Indonesia (CTI Group) salah satu penyedia solusi infrastruktur TI terbesar dan terkemuka di Indonesia Defenxor berkomitmen untuk menyediakan layanan yang andal, inovatif, dan sesuai dengan kebutuhan perkembangan teknologi saat ini.

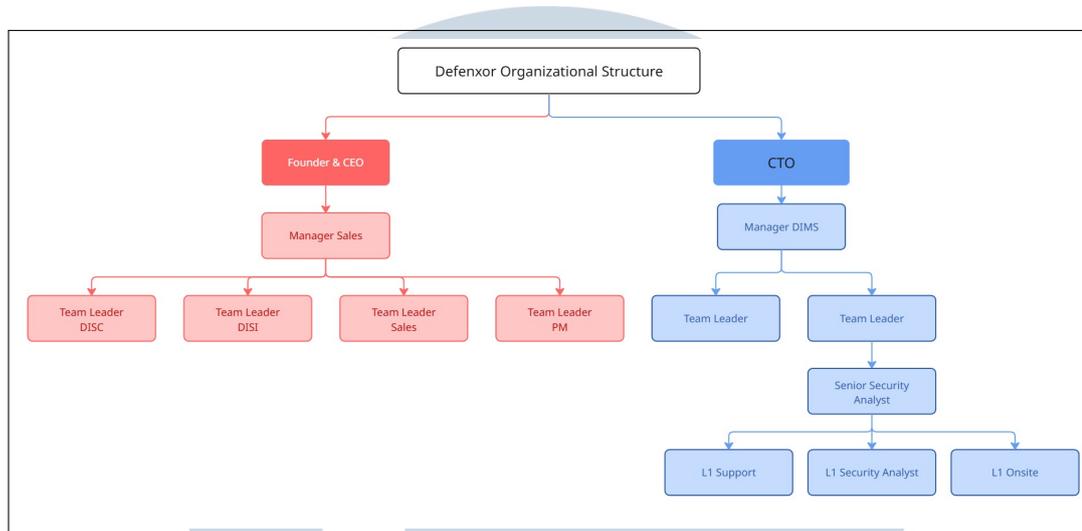
Nama Defender Nusa Semesta diambil dari kata *defender*, yang mencerminkan peran sebagai pelindung, terinspirasi dari istilah yang digunakan dalam dunia olahraga, khususnya sepak bola. Selain itu, singkatan *DNS* juga identik dengan *Domain Name System*, yang merupakan salah satu komponen fundamental dalam teknologi informasi dan sistem internet. Sementara itu, nama merek Defenxor berasal dari kata Latin *Defensor*, yang berarti pelindung atau penjaga. Merek ini dibangun berdasarkan tiga pilar utama yang menjadi dasar konsistensi dalam setiap layanan yang diberikan, sebagaimana akan dijelaskan lebih lanjut pada bagian Kompetensi Inti. ian Kompetensi Inti.

2.2 Visi dan Misi Perusahaan

Visi Defenxor adalah menjadi penyedia solusi keamanan TI terkemuka di Indonesia dan kawasan Asia Tenggara. Sebagai merek lokal yang terpercaya, Defenxor berkomitmen untuk menjadi pilihan utama bagi berbagai sektor industri dalam memenuhi kebutuhan keamanan informasi [6].

Misi Defenxor adalah menciptakan nilai tambah melalui penyediaan layanan keamanan TI profesional berkualitas tinggi dengan harga yang kompetitif. Dalam memberikan layanan, Defenxor menekankan pada keunggulan pelayanan (*service excellence*) untuk membangun kepercayaan serta menjalin hubungan jangka panjang dengan para pelanggan [6].

2.3 Struktur Organisasi Perusahaan



Gambar 2.3. Struktur organisasi perusahaan PT Defender Nusa Semesta (Defenxor)

Struktur organisasi di Defenxor dipimpin oleh seorang Chief Executive Officer (CEO) dan Chief Technology Officer (CTO). Di bawah keduanya, terdapat dua manajer yang masing-masing membawahi dua divisi, yaitu Manajer Security Operations Center (SOC) dan Manajer Sales. Selain itu, terdapat beberapa pemimpin (leader) di berbagai divisi lainnya yang mendukung kelancaran operasional perusahaan, termasuk di bidang SOC, sales, dan divisi pendukung lainnya.

PT Defender Nusa Semesta (Defenxor) menyediakan tiga layanan utama dalam bidang keamanan siber, yaitu:

2.3.1 Defenxor Intelligence Managed Security (DIMS)



Gambar 2.4. Logo DIMS

Defenxor Intelligence Managed Security (DIMS) merupakan layanan yang dirancang untuk menyederhanakan manajemen keamanan TI bagi perusahaan.

Layanan ini menawarkan solusi terhadap tantangan keamanan informasi, termasuk kebutuhan perangkat keras khusus, keahlian profesional, dan kebijakan operasional yang terpadu untuk menciptakan perlindungan yang optimal. DIMS menghadirkan tenaga profesional berstandar tinggi guna membantu perusahaan meningkatkan postur keamanan sekaligus memaksimalkan investasi dalam teknologi keamanan.

Sebagai penyedia layanan keamanan siber, kegagalan dalam memantau sistem klien, meskipun hanya dalam waktu singkat, merupakan pelanggaran serius terhadap komitmen yang telah disepakati. Untuk menjamin kesinambungan layanan tersebut, terdapat dua pilar utama yang menjadi fondasi operasional, yaitu:

Operasional Berbasis Sistem Kerja Bergilir (Shifting)

Untuk memastikan bahwa pemantauan terhadap sistem klien berjalan tanpa henti, perusahaan menerapkan sistem kerja bergilir (*shifting*) yang dirancang secara sistematis dan terstruktur. Adapun pengaturannya sebagai berikut:

- **Pembagian Waktu:** Terdapat tiga jadwal kerja yang membagi waktu selama 24 jam penuh, yaitu shift *Early*, *Mid*, dan *Late*.
- **Pembagian Hari:** Tim dibagi menjadi dua kelompok dengan pola rotasi mingguan, yaitu "*Sayap Kiri*" dan "*Sayap Kanan*", untuk memastikan cakupan pengawasan selama tujuh hari penuh, termasuk akhir pekan dan hari libur nasional.

Struktur kerja ini dirancang untuk memastikan tidak adanya kekosongan dalam proses pemantauan, sehingga setiap peringatan atau insiden yang muncul dapat segera ditangani kapan pun waktu kejadiannya.

Infrastruktur yang Andal dan Tahan terhadap Gangguan Listrik

Dalam operasional Security Operations Center (SOC), keberlangsungan layanan tidak boleh terganggu oleh faktor eksternal seperti pemadaman listrik. Oleh karena itu, perusahaan wajib menyediakan infrastruktur yang andal untuk mengantisipasi kondisi tersebut, sesuai dengan standar industri bagi penyedia *Managed Security Service Provider (MSSP)*. Infrastruktur tersebut meliputi:

- **Uninterruptible Power Supply (UPS):** Perangkat ini berfungsi untuk menyediakan pasokan listrik cadangan secara otomatis ketika terjadi pemadaman listrik utama. UPS memberikan waktu yang cukup bagi sistem untuk melakukan transisi ke sumber daya cadangan tanpa mengalami penghentian operasional secara tiba-tiba (*shutdown*).

- **Generator Set (Genset):** Untuk mengantisipasi pemadaman listrik dalam durasi yang lebih lama, genset disiapkan sebagai sumber daya utama pengganti. Genset ini mampu menyediakan suplai listrik yang mencukupi bagi seluruh perangkat penting di dalam SOC, termasuk server, perangkat jaringan, dan komputer analis, selama berjam-jam hingga sehari-hari.

Kombinasi antara UPS dan genset menjadi jaminan bahwa layanan pemantauan keamanan siber tetap berjalan normal tanpa gangguan, sekalipun terjadi permasalahan listrik dari pihak eksternal. Dengan demikian, komitmen perusahaan dalam menjaga keamanan aset digital klien dapat terus terjaga secara optimal.

Berikut adalah layanan utama yang disediakan oleh DIMS:

1. Perlindungan Sepanjang Waktu (24x7x365)
2. Pusat Operasi Keamanan Lanjutan (SOC)
3. Manajemen dan Respon Insiden
4. Perangkat Defenxor
5. Teknologi yang Sangat Tersentralisasi
6. Aplikasi Mobile Real-Time
7. Paket Layanan

2.3.2 Defenxor Intelligence Security Consulting (DISC)



Gambar 2.5. Logo DISC

Defenxor Intelligence Security Consulting (DISC) adalah layanan konsultasi keamanan yang dirancang untuk membantu bisnis memahami dan meningkatkan

keamanan sistem mereka. DISC bertujuan memastikan apakah sistem yang digunakan memenuhi standar keamanan yang dibutuhkan serta mematuhi regulasi yang berlaku.

Berikut adalah layanan yang disediakan oleh DISC:

1. Pengembangan Kebijakan Keamanan
2. Pemeriksaan Keamanan
3. Audit Keamanan
4. Sertifikasi Keamanan
5. Bantuan IT Security
6. *Penetration & Compromised Testing*

2.3.3 Defenxor Intelligence Security Integrator (DISI)



Gambar 2.6. Logo DISI

Defenxor Integrated Security Infrastructure (DISI) merupakan solusi yang memudahkan perusahaan untuk menambahkan perangkat keras keamanan tanpa harus mengeluarkan biaya besar (*CAPEX*) di awal. Dengan program pembayaran bertahap yang ditawarkan, investasi terhadap perangkat keras keamanan dapat dialihkan menjadi pengeluaran operasional (*OPEX*), sehingga pengembalian investasi (*ROI*) dapat tercapai secara optimal.

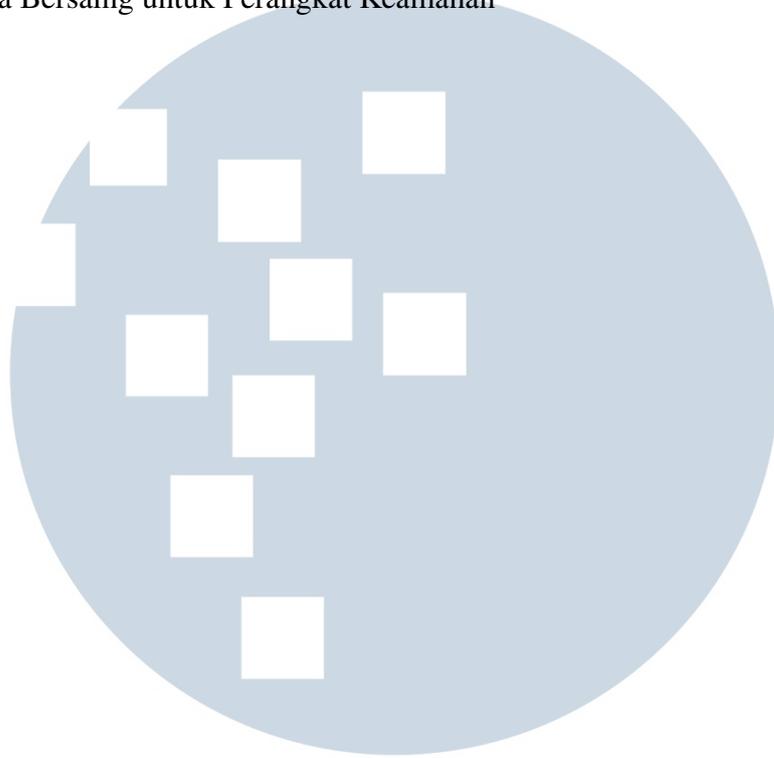
Selain itu, DISI juga menyediakan layanan *managed security*, yang menyatukan perangkat keras dan pemantauan keamanan, memberikan solusi yang terjangkau dan mudah dikelola agar perusahaan dapat fokus pada aspek bisnis lainnya.

Berikut adalah layanan yang disediakan oleh DISI:

1. Program Pembayaran Bertahap untuk Perangkat Keamanan

2. *Managed Services* Tambahan

3. Harga Bersaing untuk Perangkat Keamanan



UMMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA