



KEWIRAUSAHAAN

BUSINESS S-FUNK

KELOMPOK 7

**DOSEN PENGAMPU:
Ratna Aisuwarya, M.Eng**



ANGGOTA



01 Abil Rahman
2211511013

02 Muhammad Fadhli
2211512001

03 Fresinendi
2211512019

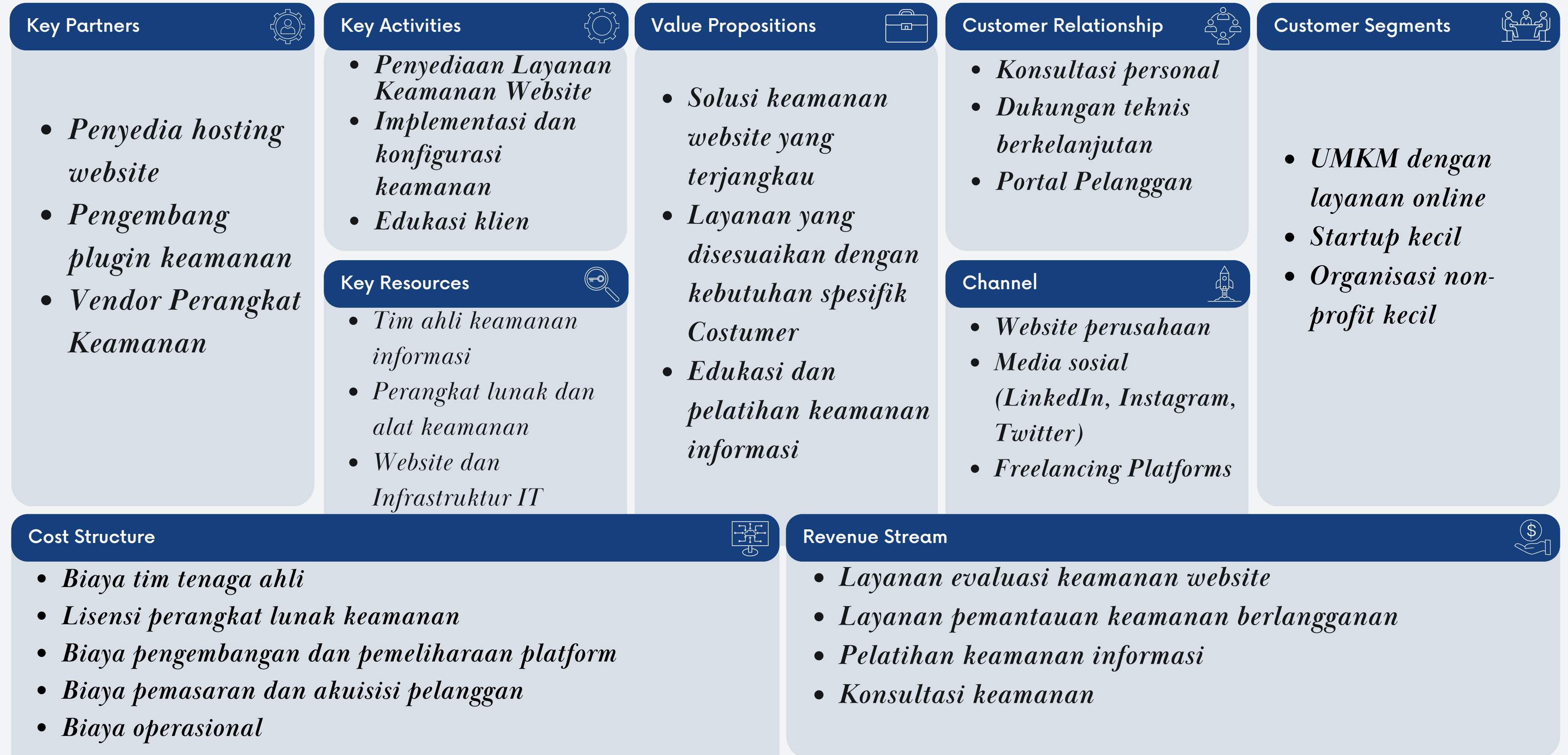
04 Daud Kurniawan
2211512021

05 Rayhan Assiddiqqy Lionar
2211513021

BUSINESS MODEL CANVAS

ide bisnis: cyber Security

S-Funk Security



KEY PARTNERSHIP

Penyedia Hosting Website

Penyedia hosting yang terpercaya mendukung infrastruktur digital yang aman, memastikan layanan keamanan berjalan lancar dan meningkatkan kepercayaan pelanggan.

Pengembang Plugin Keamanan

Dapat menyediakan solusi tambahan untuk mendeteksi ancaman, mencegah serangan, dan memperkuat sistem, sehingga perusahaan dapat menawarkan layanan yang lebih komprehensif dan adaptif.

Vendor Perangkat Keamanan

Dapat memastikan perusahaan jasa keamanan memiliki akses ke teknologi terbaru dan berkualitas, sehingga dapat memberikan layanan perlindungan yang optimal.

VALUE PROPOSITIONS



Solusi keamanan website yang terjangkau

Ini merupakan nilai utama yang ditawarkan agar solusi yang dirancang mudah dipahami dan diimplementasikan oleh klien yang tidak memiliki keahlian teknis mendalam



Layanan yang disesuaikan dengan kebutuhan spesifik

Pemberian layanan yang disesuaikan dengan kebutuhan utama bukan pendekatan one-size-fits-all



Edukasi dan pelatihan keamanan informasi

Perlunya pemberian edukasi yang menjadi komponen kunci untuk membantu klien memahami pentingnya keamanan informasi



Perlindungan data pelanggan

Merupakan tujuan akhir dari bisnis ini dimana menjaga data pelanggan dan reputasi bisnis mereka



CUSTOMER SEGMENT



UMKM dengan layanan online

Bisnis seperti toko ritel, kafe, restoran dan penyedia jasa yang sering kali memiliki infrastruktur IT yang terbatas dan rentan terhadap ancaman keamanan cyber



Stratup kecil

Perusahaan startup yang mengandalkan platform digital untuk operasi harian, tetapi mungkin saja belum memiliki sistem keamanan yang kuat



Organisasi non-profit kecil

Lembaga yang tidak berorientasi pada suatu keuntungan yang biasa beroperasi dalam skala kecil, kebanyakan bertujuan kemanusiaan, seperti yayasan sosial

CHANNELS



Website Perusahaan

Website memungkinkan perusahaan menjelaskan layanan, menampilkan testimoni dan portofolio, serta membangun kepercayaan untuk menarik lebih banyak klien.



Media sosial (LinkedIn, Instagram)

Media sosial dapat cepat menjangkau audiens luas, menunjukkan keahlian dan keandalan, serta membangun kepercayaan dan interaksi melalui konten edukatif, testimoni, dan demo layanan.



Freelancing Platforms

memungkinkan akses cepat ke tenaga ahli, menampilkan keahlian, proyek sebelumnya, dan membangun reputasi untuk menarik klien yang membutuhkan layanan keamanan khusus.



REVENUE STREAM



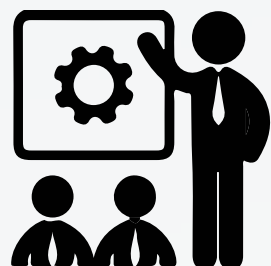
Layanan evaluasi keamanan website

Perusahaan mengenakan biaya untuk menilai dan memperbaiki kerentanan situs web klien, menghasilkan pendapatan tambahan sambil membantu melindungi data dan menghindari serangan siber.



Layanan pemantauan keamanan berlangganan

Perusahaan mengenakan biaya berulang untuk pemantauan sistem klien, memastikan perlindungan berkelanjutan dan pendapatan stabil.



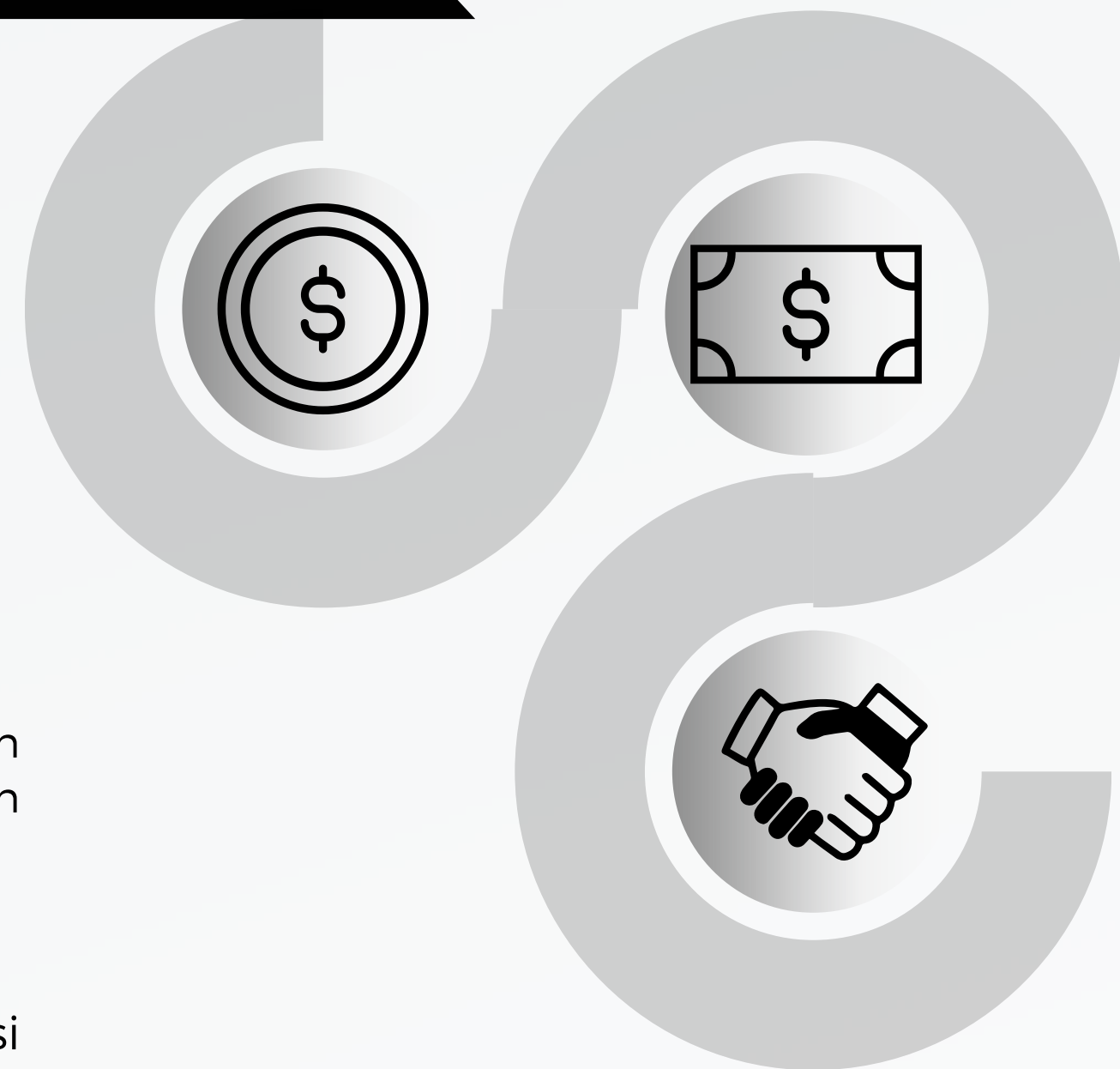
Pelatihan keamanan informasi

Perusahaan mengenakan biaya untuk pelatihan keamanan, membantu klien meningkatkan keterampilan dan kesadaran mereka, serta menghasilkan pendapatan tambahan.

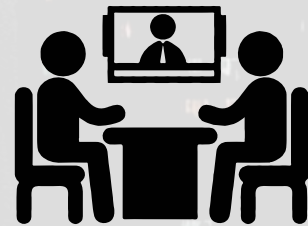


Konsultasi keamanan

Perusahaan mengenakan biaya untuk memberikan saran dan solusi keamanan yang disesuaikan, membantu klien mengatasi risiko dan meningkatkan sistem keamanan.



CUSTOMER RELATIONSHIP



Konsultasi Personal

bertujuan untuk memberikan solusi keamanan yang spesifik dan disesuaikan dengan kebutuhan individu atau perusahaan.



Dukungan Teknis

berfokus pada menjaga kinerja sistem keamanan melalui pemeliharaan rutin, pemantauan, serta bantuan teknis 24/7 untuk mengatasi masalah yang mungkin timbul



Portal Pelanggan

sarana yang memudahkan pelanggan untuk memantau status sistem keamanan, serta mengakses laporan dan pembaruan sistem secara mandiri

KEY ACTIVITIES

Penyediaan layanan Keamanan Website

Layanan ini meliputi pemantauan, deteksi, dan pencegahan ancaman seperti serangan siber dan pencurian data, serta penerapan protokol keamanan dan pembaruan sistem berkala. Tim keamanan juga bertanggung jawab merespons insiden dan mengelola risiko agar website tetap aman dan optimal.



Implementasi dan konfigurasi keamanan

Aktivitas ini meliputi pemasangan dan pengaturan sistem keamanan untuk melindungi infrastruktur digital dari ancaman siber, termasuk konfigurasi firewall, enkripsi data, dan manajemen akses. Tim keamanan memastikan semua komponen berjalan sesuai standar untuk mencegah celah keamanan.



Edukasi klien

meningkatkan kesadaran klien tentang risiko keamanan digital melalui pelatihan, workshop, dan simulasi serangan siber. Klien belajar mencegah ancaman, menangani insiden, serta mengadopsi kebijakan dan standar keamanan yang lebih baik untuk melindungi aset digital mereka.



KEY RESOURCES

01

Tim Ahli Keamanan Informasi

adalah tim yang ahli dalam cybersecurity dan manajemen risiko digital. dapat melindungi data pelanggan dari serangan siber, serta memberikan solusi terbaik dalam perlindungan informasi

02

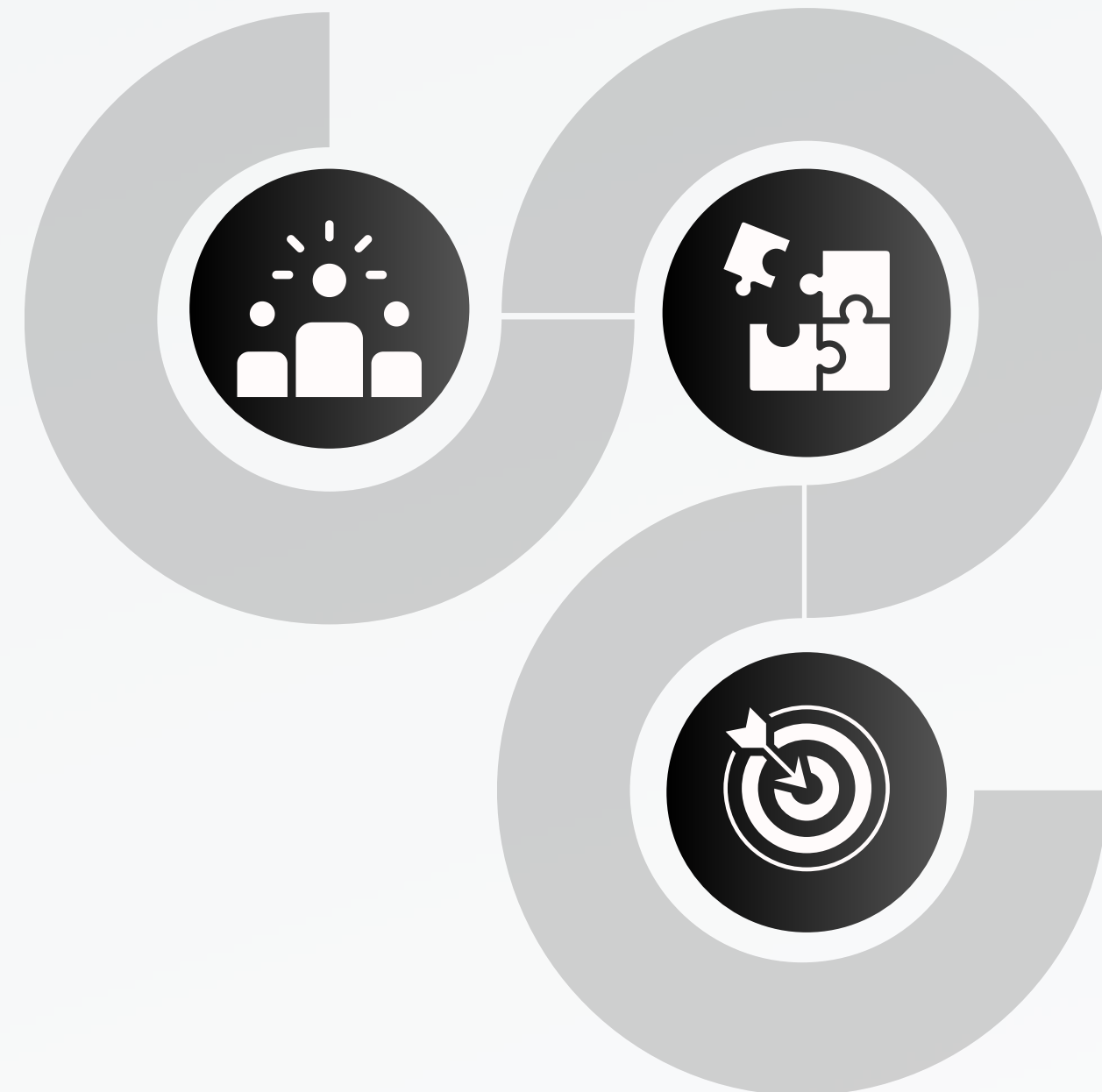
Perangkat lunak dan alat keamanan

Perangkat dan alat yang digunakan yaitu mencakup sistem keamanan digital seperti web application firewall, penetration testing tools, encryption tools, dan lain-lain.

03

Website dan Infrastruktur IT

Berfungsi sebagai sarana bagi pelanggan untuk memantau sistem keamanan mereka secara real-time.



COST STRUCTURE

Biaya tim tenaga ahli

★★★★★

meliputi gaji, pelatihan, dan sertifikasi profesional seperti analis keamanan dan insinyur jaringan, untuk merancang, mengimplementasikan, dan memelihara solusi keamanan serta memastikan kompetensi menghadapi ancaman terbaru.

Biaya pemasaran dan akuisisi pelanggan ★★★★★

Biaya pemasaran dan akuisisi pelanggan mencakup pengeluaran untuk strategi pemasaran, iklan, kampanye promosi, serta pengelolaan hubungan pelanggan seperti penawaran khusus dan program loyalitas. Investasi ini penting untuk menarik klien baru, meningkatkan kepuasan, dan memperluas pangsa pasar.

Lisensi perangkat lunak keamanan

★★★★★

mencakup pembelian dan pemeliharaan untuk alat seperti antivirus dan firewall, memastikan akses ke fitur terbaru, dukungan teknis, dan pembaruan untuk melindungi sistem dan data klien.

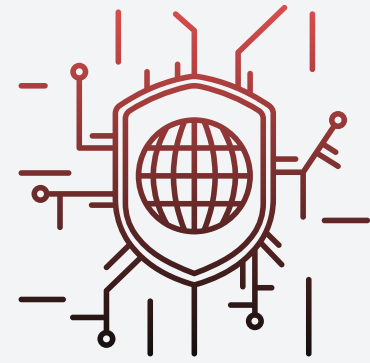
Biaya pengembangan dan pemeliharaan platform ★★★★★

mencakup pengeluaran untuk merancang, membangun, dan memperbaiki perangkat lunak serta sistem keamanan, guna memastikan platform tetap efektif dan aman terhadap ancaman siber terbaru.

Biaya operasional

★★★★★

mencakup pengeluaran rutin seperti sewa kantor, utilitas, gaji staf non-teknis, dan administrasi, yang penting untuk kelancaran dan keberlangsungan bisnis.



KELOMPOK 7

