

# YUKMARI PROJECT INDONESIA

DOCUMENT OF PARTNERSHIP / OUTSOURCING  
FOR PENETRATION TESTING & CYBER SECURITY  
(RED TEAMING & BLUE TEAMING)

# Daftar Isi

Latar Belakang	01
Tujuan Partnership	02
Benefit Partnership	03
Jenis Partnership	04
Ruang Lingkup dan Cakupan Layanan	05
Daftar Harga Layanan	06
Timeline dan Milestones	08
Risiko dan Kepatuhan	10
Penanganan Kerahasiaan dan Penanganan Data	11
Dukungan dan Pemeliharaan	12
Pengalaman Kami dan Sumber Daya	13



PT. Yuk Mari Project Indonesia, atau disingkat YMP, adalah perusahaan yang salah satunya bergerak di bidang pengembangan teknologi dan keamanan siber. Kami memiliki keahlian dalam memberikan **layanan Penetration Testing kepada perusahaan-perusahaan yang berfokus pada pengembangan aplikasi**. Melalui layanan kami, kami berkomitmen untuk membantu perusahaan Anda dalam memastikan bahwa aplikasi yang dikembangkan aman dan bebas dari potensi kerentanannya.

Yuk-Mari Project sendiri, awalnya merupakan media perkumpulan yang dirintis oleh mahasiswa Kota Bandung dari kampus ternama seperti ITB, UIN SGD, UPI, UNPAD. Kami bertujuan untuk membantu masyarakat serta pelajar dalam meningkatkan kualitas dan kapasitas mereka, baik dalam bidang teknologi maupun non-teknologi, melalui berbagai program yang kami tawarkan. Program-program tersebut antara lain **Virtual Classroom, Komunitas Siber, Konsultan Akademik, Magang/Internship, Bimbingan Belajar Online, Bimbingan Belajar Offline, Product Yuk-Mari Project, Project Program (DevApp / DevSec), dan Bootcamp Cyber Security**.

Sejak pertama kali didirikan, Yuk-Mari Project telah mengalami beberapa pengembangan, dimulai dari Yuk-Mari Kuliner (2020 - 2022), lalu berkembang menjadi Yuk-Mari Indonesia (2022 - 2023), dan saat ini menjadi Yuk-Mari Project Indonesia (2023 - sekarang). Pada tahun 2024, Yuk-Mari Project menetapkan legalisasi hukum dengan nomor **AHU-055747.AH.01.30.Tahun 2024** dan **PSE Kominfo : 015659.01/DJAI.PSE/09/2024**.

Kami memiliki visi dan misi untuk memberikan layanan berkualitas, mengikuti perkembangan teknologi terbaru, serta **memupuk hubungan jangka panjang dengan klien kami, menjadikan kami mitra yang dapat diandalkan** dalam berbagai situasi. Kami memfasilitasi pelajar, mahasiswa, dan instansi pendidikan lainnya dalam kebutuhan mereka yang bersinergi dengan program-program yang ada di Yuk-Mari Project.



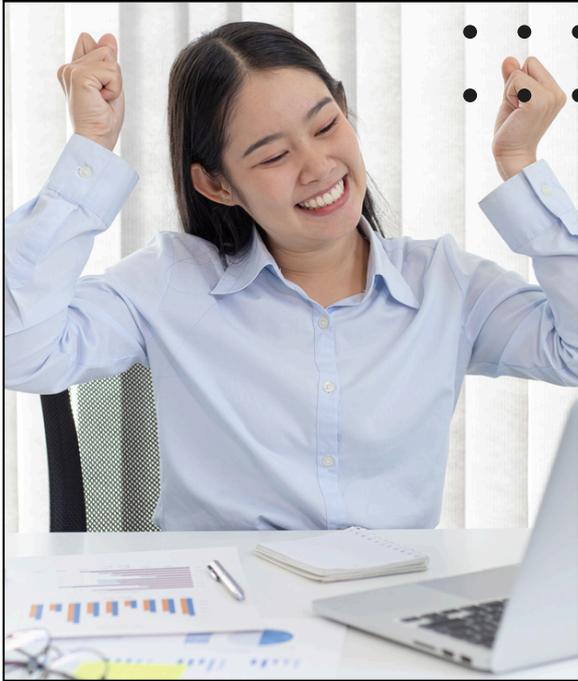
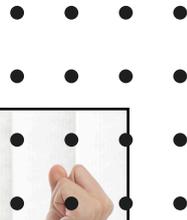
# TUJUAN PARTNERSHIP

Partnership ini bertujuan untuk menawarkan layanan **Penetration Testing** dan **Audit Keamanan Aplikasi** yang berfokus pada perlindungan jangka panjang terhadap aplikasi dan sistem yang dikembangkan oleh perusahaan.



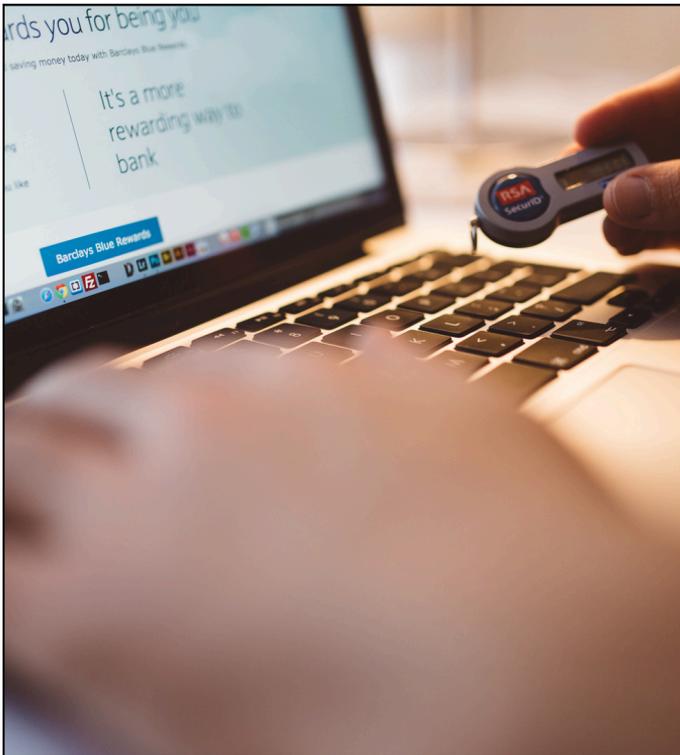
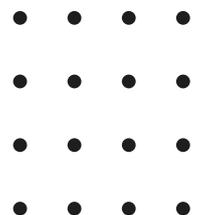
Kami berharap dapat menjalin kerjasama berkelanjutan dalam bentuk **perjanjian kontrak jangka panjang** yang mencakup **pemantauan dan pengujian keamanan** secara rutin, guna memastikan bahwa aplikasi Anda tetap aman dan bebas dari ancaman serta kerentanannya, seiring dengan berkembangnya teknologi dan potensi risiko baru.

# BENEFIT PARTNERSHIP



Dengan menggunakan layanan **Penetration Testing** dari Yukmari Project, perusahaan Anda akan mendapatkan:

- 1.Keamanan Aplikasi yang Terjamin:** Meningkatkan tingkat keamanan aplikasi dan data pengguna.
- 2.Pengurangan Risiko Keamanan:** Mengurangi potensi eksploitasi dan ancaman keamanan.
- 3.Kepatuhan terhadap Regulasi:** Memastikan aplikasi memenuhi standar dan regulasi keamanan yang relevan.
- 4.Laporan Rinci dan Solusi Perbaikan:** Menyediakan laporan komprehensif dengan langkah-langkah perbaikan untuk mengatasi temuan.



# JENIS PARTNERSHIP

## I. PROJECT-BASED

**Maksud:** Partnership Project-Based merupakan bentuk kemitraan yang bersifat sementara dan terfokus pada satu atau beberapa aktivitas spesifik dalam jangka waktu terbatas. Partnership dilakukan berdasarkan proyek tertentu yang telah disepakati. Tim kami akan bekerja berdasarkan scope, timeline, dan deliverables yang telah ditentukan sebelumnya. Setelah proyek selesai dan hasil diserahkan dalam bentuk laporan dan rekomendasi, kerja sama dinyatakan berakhir kecuali ada perpanjangan atau proyek lanjutan.

### Prefer untuk :

1. Application atau Infrastructure yang baru di rilis / peluncuran sistem / aplikasi
2. Existing Application yang ingin di audit

## II. CONTRACT-BASED

**Maksud:** Partnership Contract-Based bersifat jangka panjang dan strategis, dituangkan dalam dokumen legal seperti **Non-Disclosure Agreement (NDA)** atau **Memorandum of Understanding (MoU)**. mengatur hubungan jangka panjang antara penyedia jasa dan klien, Hal ini mencakup aspek kerahasiaan data, ruang lingkup layanan berulang atau berkelanjutan (*misalnya monitoring, incident response, konsultasi keamanan*), dan komitmen SLA (*Service Level Agreement*).

### Prefer untuk :

1. Keamanan yang kompleks dan terus berubah
2. Sistem yang perlu di jaga keamanan sistemnya (berkelanjutan)

# RUANG LINGKUP & CAKUPAN LAYANAN

Layanan yang kami tawarkan mencakup **Penetration Testing** pada Aplikasi web, aplikasi mobile, sistem jaringan internal dan eksternal, serta audit konfigurasi cloud. Kami juga menyediakan **Vulnerability Assessment** untuk mengidentifikasi potensi celah dan risiko dalam infrastruktur IT perusahaan Anda, meliputi:

- **Penetration Testing** : Aplikasi web, aplikasi mobile, jaringan internal, dan eksternal
- **Vulnerability Assessment** : terhadap sistem yang ada / *existing application*
- **Pengujian Keamanan Cloud** : (AWS, Azure, GCP) dan sistem IoT yang relevan.

## Portofolio Pentest Yang Sudah Kami Lakukan

### J&T Express Indonesia

Perusahaan di bidang industri pengiriman ekspres  
Kerentanan Utama: Shipping Rate Discount Up to 99%

### Cerebrum

Platform Try Out SNBT/UTBK  
Kerentanan Utama: Unlimited Tryout Premium Tanpa Bayar

### Kirimin Aja

Platform Aplikasi COD Semua Ekspedisi  
Kerentanan Utama: Bypass Verification Register menggunakan Fake KTP (Editing NIK + Nama)

### SiCepat Express

Layanan pengiriman di seluruh Indonesia  
Kerentanan Utama: Kebocoran Data pada Data Employee

### Bisa.AI

Platform pembelajaran digital  
Kerentanan Utama: Modifikasi Nilai Quiz (Nilai 100) per Silabus di Academy. Bisa.Network

### Rupa.AI

Media Ubah Foto dengan Teknologi AI  
Kerentanan Utama: Illegal Akses Form Upload Photo Headshot (Tanpa Bayar)

# DAFTAR HARGA LAYANAN

## I. Harga Project-Based (One-Time Services)

No	Jenis Layanan	Deskripsi Singkat	Estimasi Durasi	Harga (IDR)
1	Penetration Testing Web App / API	Pengujian blackbox + laporan temuan & rekomendasi	2-3 minggu	Rp 8.200.000,-
2	Penetration Testing Mobile App	Pengujian blackbox + laporan temuan & rekomendasi	2-3 minggu	Rp 8.200.000,-
3	Vulnerability Assessment	Pemindaian celah sistem + laporan CVSS	2-3 minggu	Rp 5.000.000,-
4	External Network Penetration Testing	Simulasi akses dari luar + laporan celah & rekomendasi	2-3 minggu	Rp 7.000.000,-
5	Internal Network Penetration Testing	Uji dari jaringan internal + mapping privilege & celah	3 minggu	Rp 9.000.000,-
6	Wireless Network Penetration Testing	Pengujian Wi-Fi + eksploitasi konfigurasi & enkripsi	1-2 minggu	Rp 6.000.000,-
7	Cloud Penetration Testing	Uji IAM & konfigurasi cloud + laporan resiko & saran	2-3 minggu	Rp 9.500.000,-

*\*Harga dapat bervariasi tergantung kompleksitas sistem dan ruang lingkup proyek.*

# DAFTAR HARGA LAYANAN

## II. Harga Contract-Based (Outsourcing / Jangka Panjang)

No	Posisi / Keahlian	Pengalaman	Deskripsi Tugas	Durasi Minimum	Biaya Per Bulan
1	Network Security Engineer	3 Tahun	Maintenance & pemantauan keamanan jaringan	6 bulan	Rp 8.000.000,-
2	SOC Analyst (L1)	2 Tahun	Monitoring log, triage alert, reporting	6 bulan	Rp 7.500.000,-
3	Penetration Tester (In-House)	3-4 Tahun	Testing internal, external app	12 bulan	Rp 10.000.000,-
4	Cyber Security Engineer	5 Tahun	Implementasi EDR, hardening, incident response	12 bulan	Rp 11.500.000,-

*\*Biaya bulanan belum termasuk PPN (jika berlaku). Durasi kontrak dapat dinegosiasikan.*

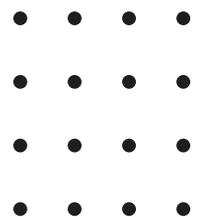
# TIMELINE DAN MILESTONES

08

## I. Milestones Schema untuk Project-Based

No	Tahapan	Estimasi Durasi
1	Kickoff & Penentuan Skop	1-2 hari
2	Pelaksanaan Pengujian	5-10 hari kerja
3	Penyusunan & Penyampaian Laporan	3-5 hari kerja
4	Re-test & Laporan Final (Opsional)	3-5 hari kerja

*\*Waktu pelaksanaan akan disesuaikan dan disepakati bersama sebelum memulai project.*



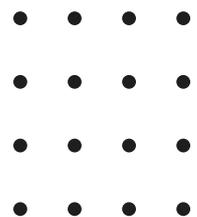
# TIMELINE DAN MILESTONES

09

## II. Milestones Schema untuk Contract-Based

No	Tahapan	Estimasi Durasi
1	Inisiasi & Perencanaan Tahunan	Awal kontrak
2	Pelaksanaan Layanan (berkala)	Bulanan / per kuartal (disepakati)
3	Laporan & Evaluasi	Setiap akhir periode layanan
4	Review Tahunan	Akhir masa kontrak

*\*Seluruh jadwal dan deliverables akan dijadwalkan bersama secara fleksibel dan dituangkan dalam kontrak kerja.*



# RISIKO DAN KEPATUHAN

## Potensi Risiko dan Penanganannya:

- 1. Gangguan Operasional:** Karena sifat pengujian penetrasi yang melibatkan serangan aktif terhadap sistem, ada kemungkinan terjadi gangguan kecil dalam operasional. Namun, kami memastikan bahwa pengujian dilakukan dalam waktu yang disepakati dan dengan izin penuh dari klien. Dapat menggunakan skema **Dev** dan **Prod**.
- 2. Potensi Dampak Keamanan:** Kami mengimplementasikan proses pengujian yang terkontrol untuk menghindari kerusakan pada sistem atau kebocoran data.

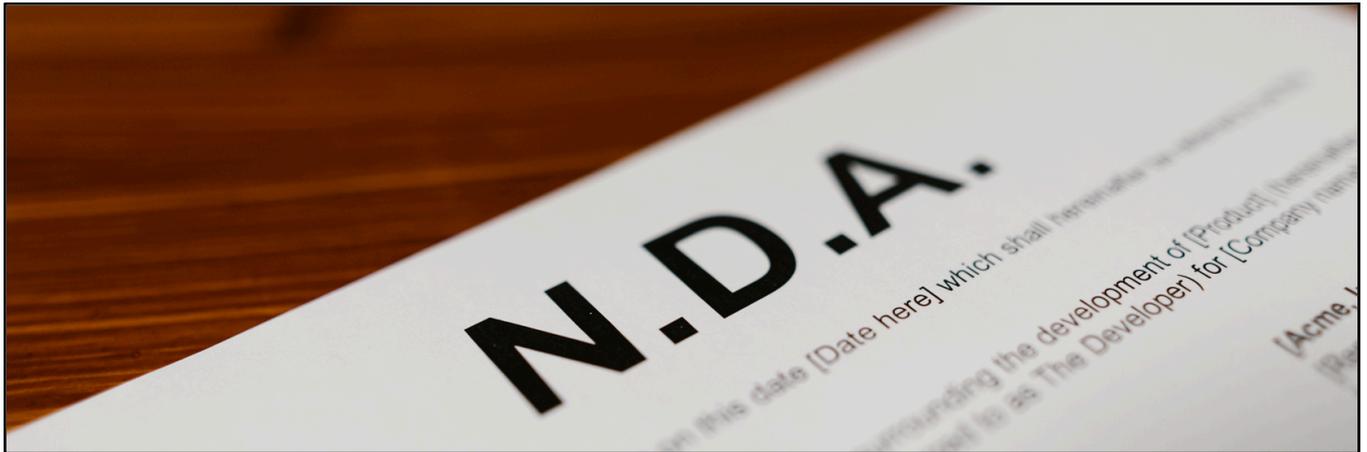
## Kepatuhan terhadap Regulasi:

Semua pengujian dilakukan dengan memperhatikan peraturan dan regulasi yang berlaku, seperti GDPR, HIPAA, PCI-DSS, dan ISO/IEC 27001, untuk memastikan bahwa Kami beroperasi dengan standar yang tinggi dan menjaga keamanan data klien.



# PENANGANAN KERAHASIAAN & KEAMANAN DATA

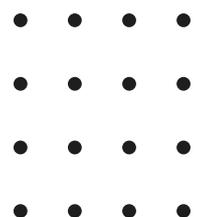
11



Kami berkomitmen untuk menjaga kerahasiaan seluruh data yang diperoleh selama pengujian. Semua temuan dan informasi terkait akan dijaga dengan standar keamanan tertinggi.

Kami menyarankan untuk menandatangani **NDA (Non-Disclosure Agreement)** untuk memastikan bahwa seluruh informasi yang terlibat dalam proses pentest tetap bersifat rahasia dan tidak akan disebarluaskan atau digunakan untuk tujuan lain.

**Keamanan Data:** Data yang diperoleh selama pengujian akan disimpan dengan enkripsi penuh dan hanya akan dibagikan kepada pihak yang berwenang dalam organisasi klien.



# DUKUNGAN DAN PEMELIHARAAN

Klien Kami mungkin memerlukan dukungan berkelanjutan setelah melakukan Penetration Test (*khusus untuk yang Project-Based*), untuk memastikan bahwa temuan telah diperbaiki dan tidak ada masalah baru yang muncul. Yang Kami lakukan:

1. **Re-test:** Kami akan melakukan re-test untuk memastikan bahwa kerentanannya telah diperbaiki sesuai dengan rekomendasi.
2. **Konsultasi Keamanan Berkelanjutan:** Tim kami siap memberikan dukungan konsultasi untuk langkah-langkah keamanan lebih lanjut dan pemantauan berkelanjutan untuk mengidentifikasi potensi risiko baru.

*\*Khusus untuk retest disesuaikan dengan metodologi project yang digunakan di lingkungan projectnya itu sendiri*

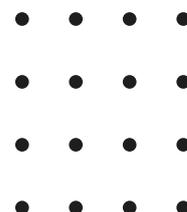
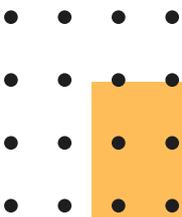


# PENGALAMAN KAMI DAN SUMBER DAYA

Kami memiliki tim yang berpengalaman dalam **penetration testing**, **auditing keamanan aplikasi**, dan **pemulihan dari serangan siber**. Tim kami mendapatkan dukungan / bantuan dari mahasiswa - mahasiswi terbaik dari kampus ternama seperti kampus PTN ataupun PTS yang dapat dilibatkan dalam berbagai aspek proyek ini sebagai bagian dari **Source**. Dan Kami telah bekerja dengan berbagai klien di sektor teknologi dan pengembangan aplikasi untuk memastikan aplikasi mereka aman dan terlindungi.



**Kegiatan CyberMeetup ke 8 - 2025  
Diselenggarakan oleh Yuk-Mari Project**





# TERIMA KASIH

Kami mengucapkan terima kasih atas waktu dan perhatian yang telah diberikan untuk meninjau proposal ini - **CEO PT. Yuk-Mari Project Indonesia**

