

دفاع سایبری میراث

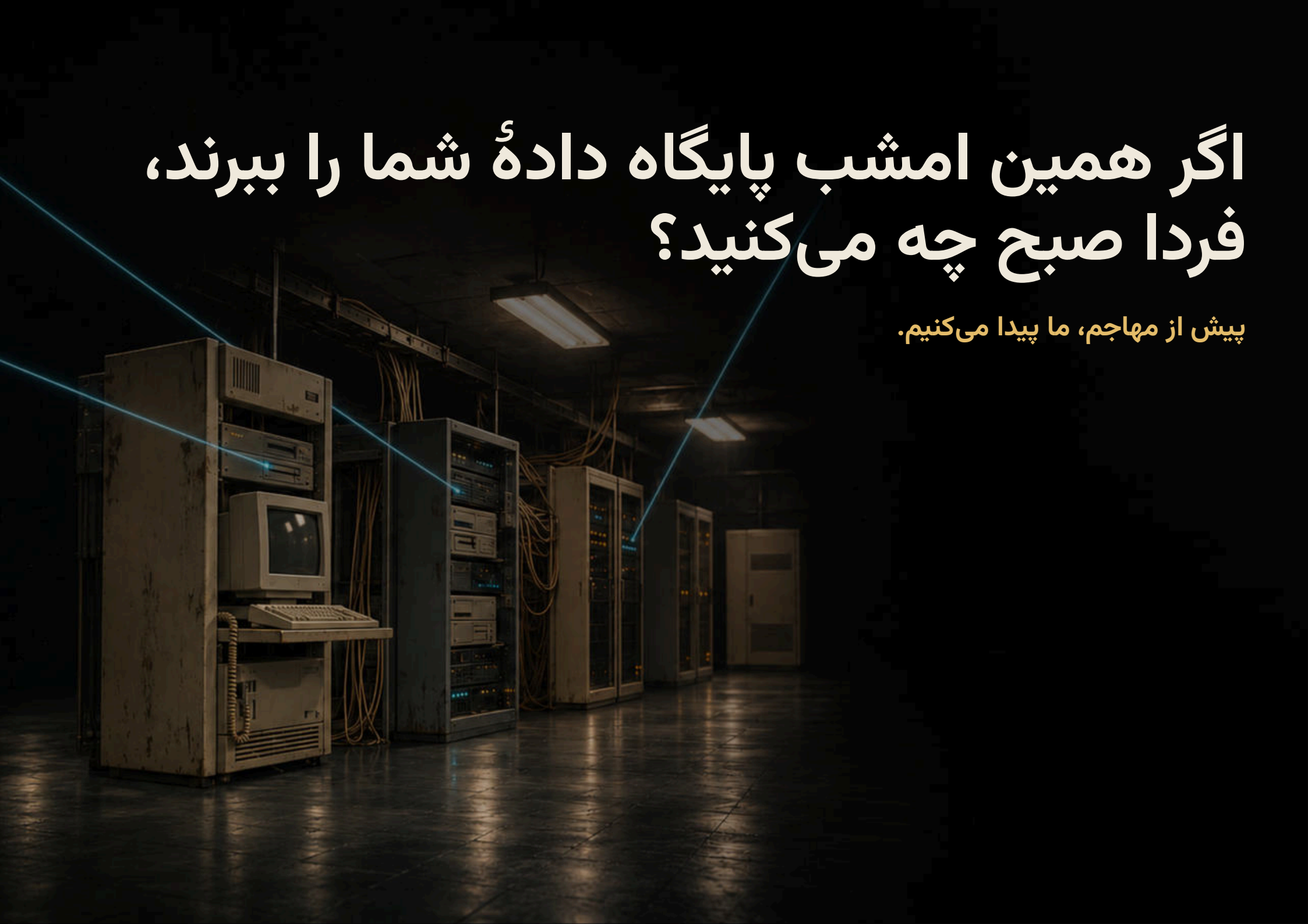
امنیت را به میراث بسپارید

دفاع سایبری مدیریت‌شده برای شرکت‌ها و گروه‌های بزرگ

حفاظت از سامانه‌های موجود، داده‌های حساس و تداوم خدمات حیاتی.

ارزیابی محرمانهٔ رایگان ←

گزارش یک‌صفحه‌ای برای هیئت‌مدیره

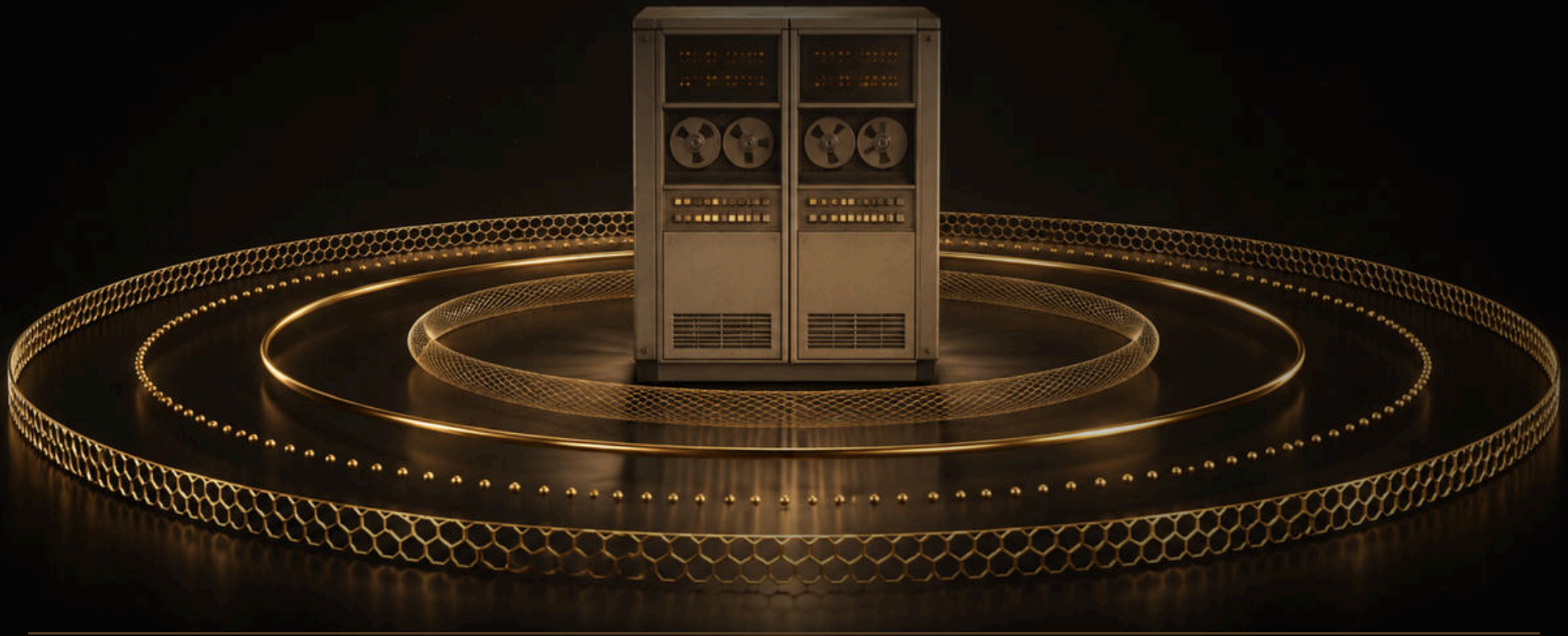


اگر همین امشب پایگاه دادهٔ شما را ببرند، فردا صبح چه می‌کنید؟

پیش از مهاجم، ما پیدا می‌کنیم.

سیستم‌هایتان قدیمی است.
امنیتشان نباید باشد.

بدون تعویض سامانه‌ها، دور آن‌ها سپر می‌کشیم.



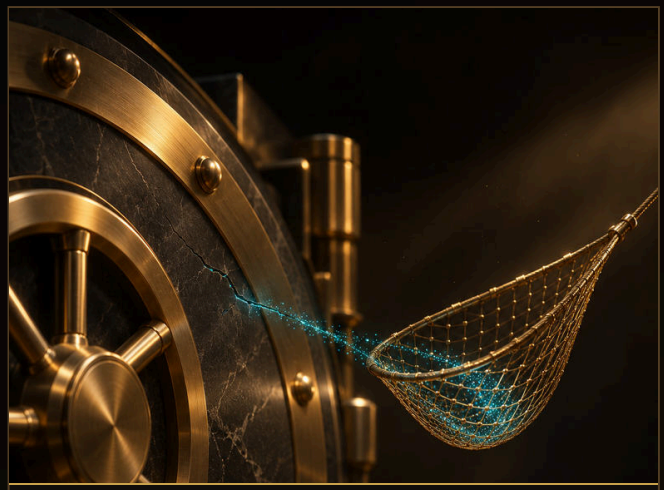
دیوار آتش برنامه (WAF)

کنترل دسترسی ممتاز (PAM)

دسترسی بدون اعتماد پیش‌فرض (Zero Trust)

پایش ۲۴ ساعته (SOC)

داده‌ها محفوظ بمانند.
خدمات حیاتی در دسترس بمانند.



نشت اطلاعات

اطلاعات مشتریان شما، امروز دست کیست؟

خطر: اطلاعات مشتری افشا می‌شود.

کار ما: انتقال داده را محدود می‌کنیم.

نتیجه: می‌دانید کدام داده کجاست و دست چه کسی است.



DDoS

سرویس شما چند دقیقه حمله را تاب می‌آورد؟

خطر: سرویس از دسترس خارج می‌شود.

کار ما: ترافیک مخرب را فیلتر می‌کنیم.

نتیجه: برای روز حمله، برنامهٔ آماده دارید.



باج‌افزار

اگر فردا همهٔ فایل‌ها قفل شود، پشتیبان شما کار می‌کند؟

خطر: فایل‌های کاری قفل می‌شوند.

کار ما: بازیابی پشتیبان را تمرین می‌کنیم.

نتیجه: پشتیبانِ آزموده دارید، نه امید.

راه‌های نفوذ را محدود کنید.
برای توقف سرویس آماده باشید.



نفوذ

آخرین تلاش برای نفوذ به شما کی بود؟

خطر: رخنهٔ وب راه ورود می‌شود.

کار ما: رخنه‌ها را برطرف می‌کنیم.

نتیجه: رخنه‌های یافته‌شده پیش از مهاجم بسته می‌شوند.



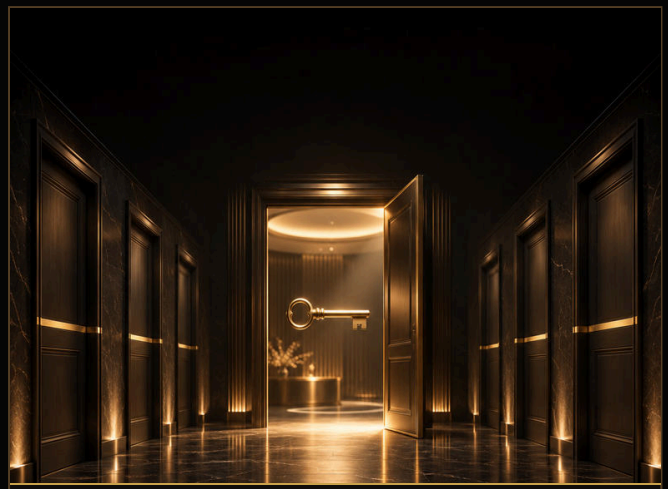
توقف سرور

سرور شما چند ساعت خاموشی را تحمل می‌کند؟

خطر: خرابی سرور کار را متوقف می‌کند.

کار ما: مسیر جایگزین را آماده می‌کنیم.

نتیجه: مسیر جایگزینِ تمرین‌شده دارید.



دسترسی

یک رمز لو رفته کافی است.

خطر: حساب کاری به خطر می‌افتد.

کار ما: ورود را محدود و ثبت می‌کنیم.

نتیجه: هر ورود نام و ردپا دارد.

یک تیم پاسخ‌گو برای دفاع سایبری

پایش، پاسخ، بازیابی و امنیت سامانه‌های هوش مصنوعی زیر نظر یک مسئول مشخص.



ارزیابی محرمانه

ریسک‌های اصلی را پیدا می‌کنیم.

اجرای مرحله‌ای

کنترل‌ها را مستقر می‌کنیم.

پایش و پاسخ

هشدارها را پیگیری می‌کنیم.

بازیابی و گزارش

بازگردانی را تمرین می‌کنیم.

چرا میراث

اتاق دادهٔ اختصاصی در تهران

داده‌های شما در ایران می‌ماند

چهار سامانهٔ NVIDIA A100 برای مدل‌های اختصاصی

دفتر دبی و دسترسی بین‌المللی

چارچوب‌های مرجع کار ما

CVSS | PTES | OWASP | NIST CSF | ISO/IEC 27001



مهاجمان امروز هوش مصنوعی دارند. دفاع شما چه دارد؟

حفاظت از داده

اطلاعاتی را که دستیار هوش مصنوعی می‌بیند محدود می‌کنیم.

کنترل اقدام عامل‌ها

برای کارهای حساس، تأیید انسان و ثبت اقدام می‌گذاریم.

آمادگی تیم

مقابله با فیشینگ و جعل صدا را تمرین می‌کنیم.

سابقهٔ اجرایی، تعهد قابل سنجش

پروژه‌های امنیت سایبری در مقیاس سازمانی، با معیارهای روشن برای تحویل و پذیرش.

پروژه‌های اجراشده

- کنترل دسترسی ممتاز
- دسترسی بدون اعتماد پیش‌فرض
- مدیریت هویت و دسترسی
- دفاع در برابر DDoS
- ورود یکپارچه و احراز چندمرحله‌ای
- مرکز عملیات امنیت
- دیوار آتش برنامه و درگاه API

تعهداتی که در قرارداد می‌آید

محرمانگی پرونده

توافق محرمانگی و تعیین مدت نگهداری اطلاعات.

زمان آغاز پاسخ

ساعات پوشش و مسیر اطلاع‌رسانی رخداد.

پذیرش اصلاحات

معیار روشن برای بررسی و تحویل اصلاحات.

بازآزمایی رایگان تا رفع کامل

در جلسهٔ محرمانه، نمونهٔ گزارش فنی و سابقهٔ مرتبط با نیاز سازمانتان را بررسی می‌کنیم.

معرفی گروه

هلدینگ میراث

گروهی ایرانی که از سال ۱۳۹۳ در حوزه‌های فناوری، صنعت، معماری، ساخت و بازرگانی فعالیت می‌کند.

حوزه‌های فعالیت

توسعه و سرمایه‌گذاری در هوش مصنوعی، معماری و طراحی، ساختمان و توسعه، بازرگانی عمومی.

سوابق هوش مصنوعی و صنعت

فولاد مبارکه، شرکت ملی صنایع مس ایران، مبین‌نت و رایتل از نام‌های معرفی‌شده در سوابق این بخش‌اند.

مشاهدهٔ سوابق هوش مصنوعی میراث ←

دفتر مرکزی تهران، فرمانیه، برج پارامیس، طبقهٔ ۷، واحد ۷۰۲

تهران، اصفهان، نوشهر و دبی

دفتر میراث ۰۲۱ ۲۲۲۲ ۹۲۲۲	واتس‌اپ ۰۹۱۲ ۳۳۳ ۳۱۰۳
ایمیل info@mirasholding.com	وب‌سایت mirasholding.com



از یک سرویس حیاتی شروع کنیم

هزینهٔ پیشگیری را شما تعیین می‌کنید.
هزینهٔ حمله را مهاجم.

ارزیابی محرمانهٔ رایگان ←

گزارش یک‌صفحه‌ای برای هیئت‌مدیره

دفتر میراث
۰۲۱ ۲۲۲۲ ۹۲۲۲

واتس‌اپ
۰۹۱۲ ۳۳۳ ۳۱۰۳

ایمیل
info@mirasholding.com

وب‌سایت
mirasholding.com

دفتر مرکزی تهران، فرمانیه، برج پارامیس، طبقهٔ ۷، واحد ۷۰۲

زیر حمله‌اید؟ همین حالا تماس بگیرید: ۰۲۱ ۲۲۲۲ ۹۲۲۲