شرکت فناوری‌های پیشرفته تبادل امن

چارچوب و استانداردها

ISO 27001 INFORMATION SECURITY

MITRE

OWASP

NIST

درباره ما ؟

شرکت **فناوری‌های پیشرفته تبادل امن** در سال ۱۴۰۱ با هدف **مقابله با تهدیدات بدافزاری و ارائه راهکارهای پیشرفته در حوزه امنیت سایبری** در سطح ملی تأسیس شد. این شرکت با رویکردی نوآورانه و مبتنی بر دانش بومی، فعالیت خود را در زمینه توسعه محصولات و خدمات امنیت اطلاعات آغاز کرد.

امروزه شرکت فناوری‌های پیشرفته تبادل امن با حضور بالغ بر ۲۳۰ نفر از متخصصان و نخبگان حوزه‌های برنامه‌نویسی، امنیت سایبری و شبکه، به یکی از مجموعه‌های در حال رشد این حوزه تبدیل شده‌است. سرمایه انسانی متخصص، اصلی‌ترین دارایی شرکت محسوب می‌شود و نقش کلیدی در توسعه محصولات و خدمات آن ایفا می‌کند.

محصولات و راهکارهای شرکت ما با نام تجاری **ققنوس** شامل **سامانه‌های پیشرفته EDR، ضدبدافزار اندرویدی، پیام‌رسان سازمانی** و سایر محصولات امنیتی است.
همچنین خدمات تخصصی تحلیل بدافزار و ارزیابی امنیتی سامانه‌های فناوری اطلاعات توسط دپارتمان‌های تخصصی شرکت ارائه می‌شود و به طور مستمر در حال توسعه و به‌روزرسانی است.

چرا ما ؟

بومی‌سازی مبتنی بر نیاز سازمان‌های ایرانی

ما در **تبادل امن**، محصولات خود را بر اساس شناخت دقیق از ساختار سازمانی، الزامات قانونی و چالش‌های امنیتی ایران طراحی کرده‌ایم. راهکارهای ما فقط نسخه‌ای ترجمه‌شده از مدل‌های خارجی نیستند بلکه هم‌راستا و هم‌سو با شرایط و محیط عملیاتی سازمان‌ها می‌باشند.

امنیت، از لحظه‌ی طراحی تا اجرا

برای ما امنیت یک قابلیت اضافه‌شده نیست؛ بلکه از نخستین مرحله طراحی در ساختار محصولات ما تنیده شده است. این رویکرد طراحی بر پایه امنیت، پایداری، یکپارچگی و مقاومت واقعی در برابر تهدیدات سایبری را تضمین می‌کند.

ترکیب تخصص عمیق با رویکرد مسئولانه

ما نگهبانی آگاه با نگاهی نوآورانه در تضمین و توسعه امنیت هوشمند هستیم. تیم متخصص ما با تجربه عملیاتی، محصولات را در تراز استانداردهای جهانی طراحی می‌کند.

کنترل‌پذیری و گزارش‌پذیری سازمانی

راهکارهای ما با فراهم‌سازی دسترسی‌های سطح‌بندی‌شده، داشبوردهای مدیریتی و گزارش‌های تحلیلی دقیق، امکان نظارت مستمر بر جریان ارتباطات و وضعیت امنیت را برای مدیران فراهم می‌کند. این شفافیت، تصمیم‌گیری سریع‌تر، مدیریت ریسک مؤثرتر و پاسخ‌گویی دقیق‌تر در شرایط حساس را ممکن می‌سازد.

تعادل میان امنیت و تجربه کاربری

بسیاری از راهکارهای امنیتی بهره‌وری را کاهش می‌دهند. در **تبادل امن**، ما این دو را در تقابل با یکدیگر نمی‌بینیم. علاوه بر طراحی ساختارمند و هوشمندانه، تمرکز بر رابط کاربری بهینه باعث می‌شود کاربران بدون احساس محدودیت، در محیطی کاملاً امن فعالیت کنند.


امنیت واقعی، حاصل یک لایه نیست؛
دفاع در چند لایه است...

امنیت شبکه

Network Security

حفاظت از زیرساخت شبکه و کنترل ترافیک ورودی و خروجی، نقشی کلیدی در پیشگیری از نفوذ و کاهش تهدیدات سایبری ایفا می‌کند. طراحی و پیاده‌سازی راهکارهای تخصصی در این حوزه، بستری امن برای مدیریت مطمئن ارتباطات داخلی و خارجی فراهم می‌آورد.

مجموعه راهکارهای ارائه‌شده توسط کارشناسان ما، شامل پیاده‌سازی فایروال‌های نسل جدید، مدیریت ترافیک، جلوگیری از نفوذ و کنترل دقیق دسترسی کاربران است.

در این مسیر، بهره‌گیری از NGFW امکان تحلیل عمیق بسته‌ها و ارتقای امنیت مرزهای شبکه را میسر می‌سازد. همچنین با استفاده از خدمات امن‌سازی و ارزیابی شبکه، نقاط ضعف، شناسایی شده و با بهبود ساختار دفاعی، پایداری زیرساخت تضمین می‌شود.

مدیریت هویت و دسترسی

Identity and Access Management

مدیریت هویت دیجیتال و کنترل دقیق دسترسی‌ها، از حیاتی‌ترین ارکان امنیتی در زیرساخت‌های مدرن به شمار می‌رود. تیم متخصص ما با طراحی و پیاده‌سازی معماری‌های پیشرفته مدیریت هویت، امنیت و انضباط عملیاتی را تضمین می‌کند.

بهره‌گیری از راهکارهای نوین نظیر احراز هویت چندمرحله‌ای، مدیریت جامع دسترسی‌ها، کنترل دسترسی‌های ویژه، یکپارچه‌سازی هویت و استقرار سیاست‌های دسترسی امن، توسط کارشناسان ارشد ما با دقت بالا اجرا می‌گردد؛ تا از سوءاستفاده‌ها و ورود غیرمجاز به داده‌های حساس، به‌طور ریشه‌ای جلوگیری شود.

امنیت کارمندان و تجهیزات

Employee and Equipment Security

تجهیزات کاربران، لپ‌تاپ‌ها، سرورها و سایر نقاط پایانی از مهم‌ترین اهداف حملات سایبری محسوب می‌شوند. محافظت مستمر از این تجهیزات نقش مهمی در کاهش سطح حمله و جلوگیری از انتشار تهدیدات دارد.

در حوزه امنیت کاربران و تجهیزات، محافظت از نقاط پایانی مانند لپ‌تاپ‌ها، سرورها و تجهیزات همراه اولویت اصلی ماست. سامانه EDR ققنوس با پایش رفتار سیستم‌ها، امنیت نقاط پایانی را تأمین می‌کند. علاوه بر این، ضدبدافزار اندرویدی ققنوس برای حفاظت از تلفن همراه و ضدبدافزار لینوکسی ققنوس جهت امنیت سرورها و عامل‌های لینوکسی طراحی شده‌اند. همچنین پیام‌رسان سازمانی قاصدک، بستری امن برای ارتباطات داخلی فراهم می‌آورد. در نهایت ما با تکیه بر خدمات تحلیل بدافزار به سازمان‌ها کمک می‌کنیم تا ماهیت تهدیدات را شناسایی کرده و راهکارهای دقیق‌تری جهت مقابله با آن‌ها پیاده‌سازی کنند.

امنیت نرم‌افزار و سرویس‌ها

Software and Services Security

بخش قابل توجهی از تهدیدات سایبری از طریق نرم‌افزارها، سرویس‌های تحت وب و آسیب‌پذیری برنامه‌ها انجام می‌شود. به همین دلیل، توجه به امنیت نرم‌افزار در تمامی مراحل طراحی، توسعه و بهره‌برداری، ضرورتی انکارناپذیر است.

در این راستا، پیاده‌سازی خدماتی نظیر ارزیابی امنیتی، تست نفوذ، بررسی دقیق کد و حفاظت از سرویس‌های تحت وب، توسط متخصصان زبده ما بستری را فراهم می‌آورد تا مخاطرات امنیتی در لایه نرم‌افزاری به شکلی محسوس کاهش یافته و سطح تاب‌آوری زیرساخت‌های حیاتی در برابر حملات سایبری ارتقا یابد.

امنیت زیرساخت

Network Infrastructure Security

طراحی صحیح معماری شبکه و کنترل ارتباطات داخلی، نقشی تعیین‌کننده در محدودسازی دسترسی مهاجمان و صیانت از دارایی‌های حیاتی ایفا می‌کند.

در حوزه امنیت داخلی زیرساخت، تمرکز بر تفکیک‌بندی شبکه، ایمن‌سازی تجهیزات و کنترل دسترسی‌های داخلی است. در این مسیر، بهره‌گیری از راهکارهای PE و SOAR و پیاده‌سازی آن توسط متخصصان خبره ما، امکان خودکارسازی پاسخ به رخدادها و افزایش هماهنگی میان سامانه‌های دفاعی را فراهم می‌سازد تا مقابله با تهدیدات با سرعت و دقت بیشتری انجام شود.

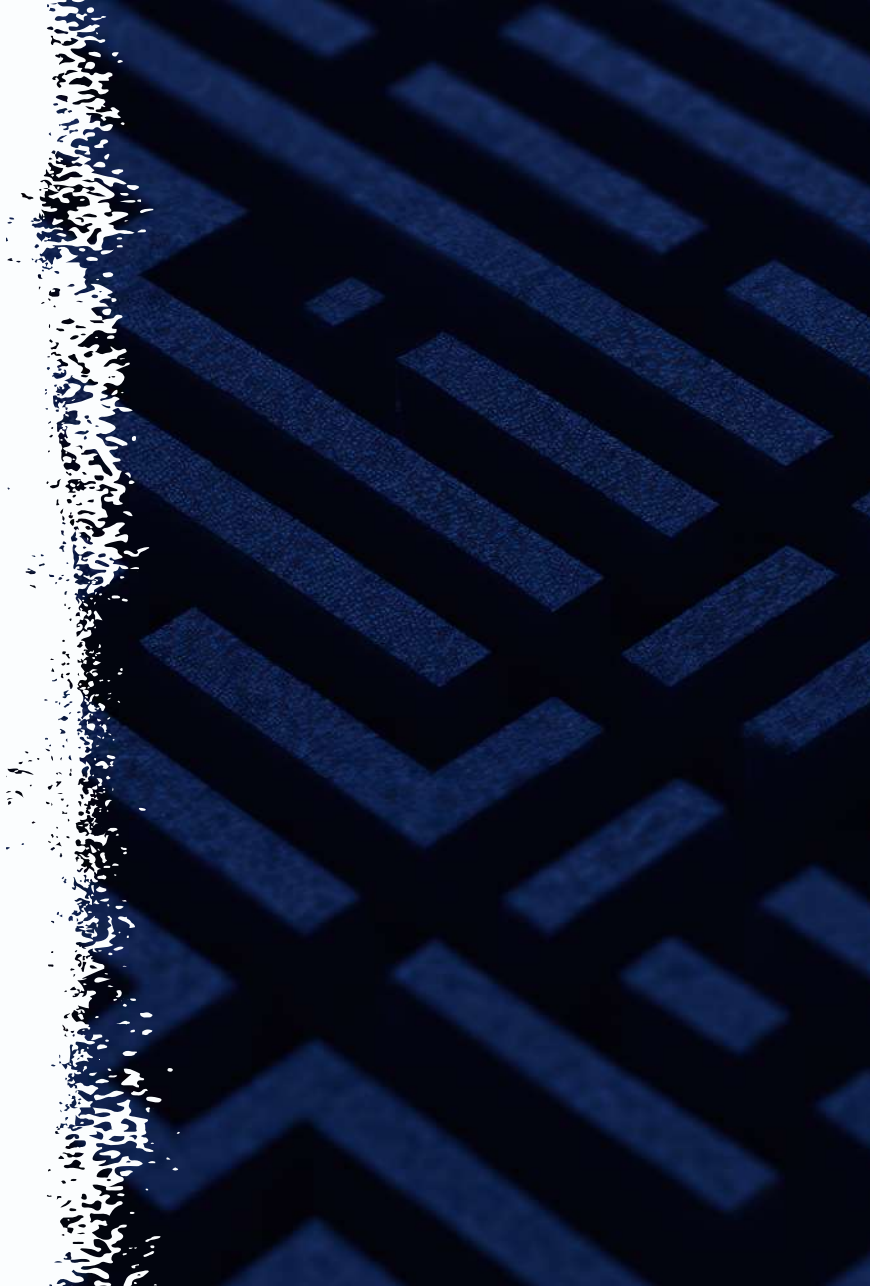
حفاظت از داده

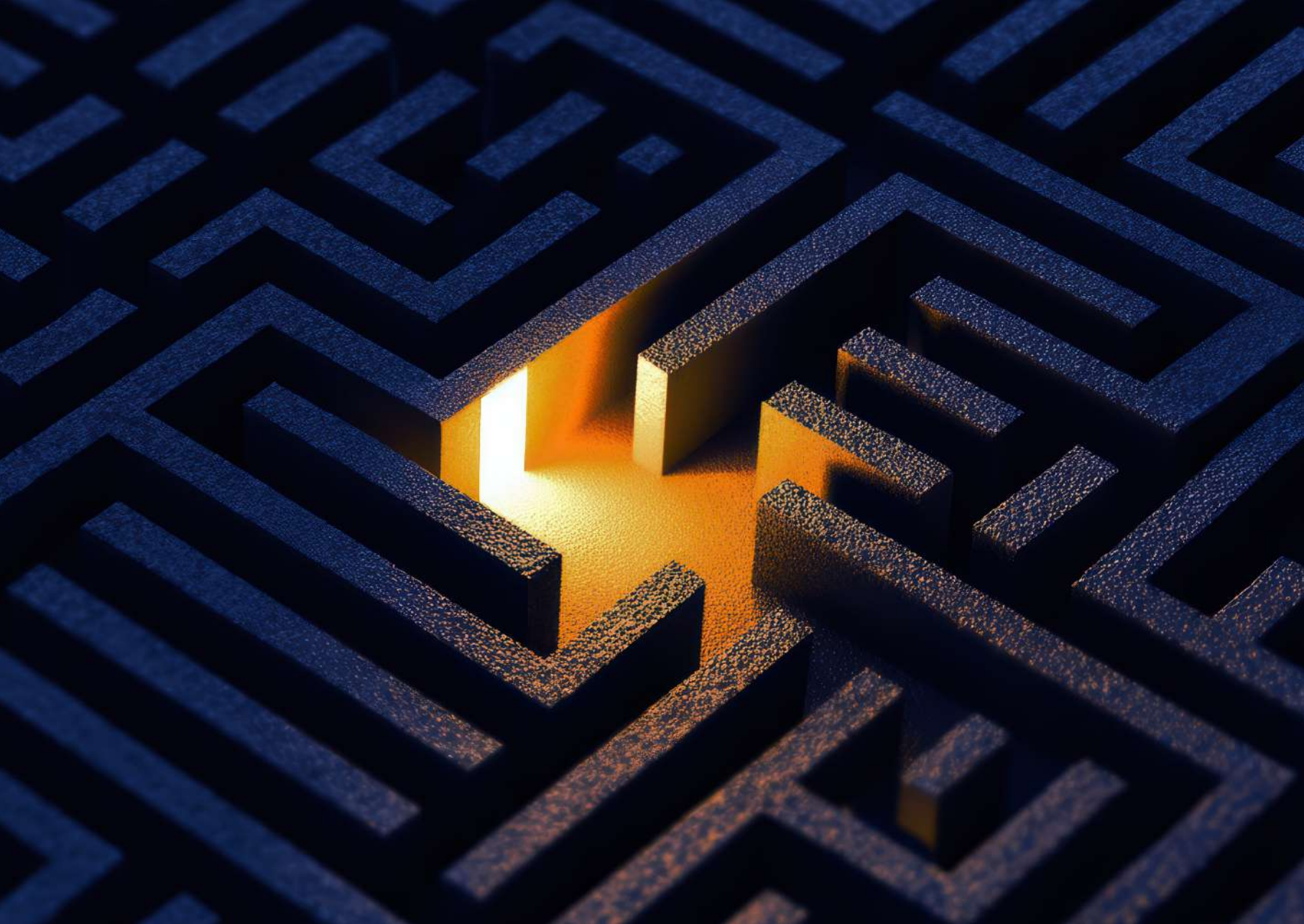
Data Security

داده‌ها به عنوان ارزشمندترین دارایی‌های هر نهاد و زیرساخت، نیازمند صیانت مستمر از اصول سه‌گانه محرمانگی، یکپارچگی و دسترس‌پذیری هستند.

استقرار راهکارهای حفاظت از داده شامل رمزنگاری اطلاعات، کنترل دقیق دسترسی‌ها، پیشگیری از نشت اطلاعات، مدیریت جامع نسخه‌های پشتیبان و قابلیت بازیابی امن، نقشی کلیدی در تضمین تداوم عملیات و حفظ سلامت دارایی‌های اطلاعاتی ایفا می‌کند.

مسیر نفوذ را به هزارتو تبدیل کن!





مدیریت رخداد و پاسخ به حملات

Incident Response

سرعت واکنش در زمان وقوع رخدادهای امنیتی، تأثیری مستقیم بر کاهش ابعاد خسارات و جلوگیری از گسترش تهدیدات دارد. طراحی فرآیندهای پاسخ‌گویی و مدیریت رخداد، امکان اقدام مقتدرانه و سریع را در زمان وقوع حملات فراهم آورده و از بروز اختلالات گسترده در حین ارائه خدمات جلوگیری می‌کند.

امنیت کاربران و فرهنگ‌سازی امنیتی

Users Safety and Security Culture

با توجه به اینکه عامل انسانی اغلب به بزرگ‌ترین آسیب‌پذیری در برابر حملات فیشینگ و مهندسی اجتماعی تبدیل می‌شود، مدیریت هوشمند دانش کاربران یک ضرورت استراتژیک است.

ما با بهره‌گیری از دانش عمیق متخصصان خود، فرآیند فرهنگ‌سازی امنیتی را از یک آموزش ساده به یک سیستم دفاعی پیشرفته ارتقا می‌دهیم.

تدوین و اجرای برنامه‌های آموزش تخصصی توسط تیم خبره ما، با هدف اصلاح رفتارهای دیجیتال و به حداقل رساندن خطاهای انسانی، تضمین‌کننده پایداری و امنیت زیرساخت‌های حیاتی در مواجهه با حملات پیچیده است.

مدیریت ریسک و ارزیابی امنیتی

Risk Assessment

شناسایی دقیق ریسک‌ها و ارزیابی مستمر وضعیت امنیتی، از حیاتی‌ترین مراحل در طراحی و استقرار راهکارهای کارآمد امنیت سایبری است.

خدمات این حوزه شامل ارزیابی‌های امنیتی، تحلیل آسیب‌پذیری‌ها، ممیزی‌های تخصصی، بررسی انطباق با استانداردها و تحلیل شکاف‌های امنیتی توسط آزمایشگاه‌های تخصصی ما می‌باشد.

امنیت ابری

Cloud Security

با گسترش روزافزون زیرساخت‌های ابری، حفاظت از داده‌ها و سرویس‌های مبتنی بر ابر، ضرورتی انکارناپذیر است.

استقرار راهکارهای امن، تضمین‌کننده محافظت از سرویس‌ها و داده‌ها در محیط‌های ابری و ارتقای سطح پایداری و امنیت زیرساخت‌هاست.

مانیتورینگ امنیت و مرکز عملیات امنیت

SOC: Security Operation Center

پایش مستمر رخدادهای امنیتی، زیربنای شناسایی سریع تهدیدات و واکنش قاطع در برابر حملات سایبری محسوب می‌گردد. استقرار سیستم‌های مانیتورینگ امنیتی، نقشی حیاتی در کاهش ابعاد خسارات و ارتقای سطح آمادگی زیرساخت‌ها در مواجهه با تهدیدات نوظهور ایفا می‌کند.

در این حوزه، ارائه خدماتی نظیر: جمع‌آوری و تحلیل جامع رخدادها، پایش لحظه‌ای امنیتی، تحلیل تهدیدات، شناسایی رفتارهای غیرعادی و مدیریت ساختارمند رخدادهای امنیتی، بستری استوار برای حفظ پایداری و امنیت محیط‌های عملیاتی فراهم می‌آورد.

حاکمیت امنیت و انطباق

Governance and Compliance Security

پیاده‌سازی چارچوب‌ها و استانداردهای بین‌المللی امنیتی نقشی کلیدی در ارتقای بلوغ امنیتی و بهبود فرآیندهای مدیریت ریسک ایفا می‌کند. تیم ما متشکل از متخصصان برجسته و کارشناسان خبره در حوزه فناوری اطلاعات، خدمات این بخش را با بالاترین سطوح کیفی ارائه می‌دهند.

این خدمات شامل: مشاوره تخصصی و استقرار استانداردهای بین‌المللی، تدوین جامع سیاست‌ها و فرآیندهای مدیریت امنیت اطلاعات و تضمین انطباق کامل با الزامات قانونی و مقرراتی است که با دقت و تسلط کامل بر استانداردهای روز دنیا اجرا می‌گردد.


برای هر ریسک، یک راهکار هوشمند

فناوری‌های پیشرفته

تبادل امن

تهران، میدان هفت‌تیر، خیابان کریمخان،
خیابان خردمند شمالی، کوچه هجدهم، پلاک ۲۱

https://tabadolamn.ir

فردای امن، از امروز آغاز می‌شود...